Contract #: AR3114

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Utah Division of Purchasing and the following Contractor:

Red River Technology LLC
Name

21 Water Street, Suite 500
Street Address

Claremont	NH	03743
City	*State*	*Zip*

Vendor # VC226567 Commodity Code #: 920-05 Legal Status of Contractor: Limited Liability Company

Contact *Name:* Dan McGee *Phone Number:* 603-442-5513 *Email:* dan.mcgee@redriver.com

2. CONTRACT PORTFOLIO NAME: Cloud Solutions.

3. GENERAL PURPOSE OF CONTRACT: Provide Cloud Solutions under the service models awarded in Attachment B.

4. PROCUREMENT: This contract is entered into as a result of the procurement process on FY2018, Solicitation# SK18008

5. CONTRACT PERIOD: Effective Date: Friday, June 28, 2019. Termination Date: Tuesday, September 15, 2026 unless terminated early or extended in accordance with the terms and conditions of this contract.

6. Administrative Fee: Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) of contract sales no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.

7. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Schedule
ATTACHMENT D: Contractor's Response to Solicitation # SK18008
ATTACHMENT E: Service Offering EULAs, SLAs

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

9. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah Procurement Code, Procurement Rules, and Contractor's response to solicitation #SK18008.

10. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed. Notwithstanding verbal or other representations by the parties, the "Effective Date" of this Contract shall be the date provided within Section 5 above.

CONTRACTOR

George Shalhoub
George Shalhoub (Jun 27, 2019)
Contractor's signature

Jun 27, 2019
Date

George Shalhoub
Type or Print Name and Title

Director of Contract Admin.

DIVISION OF PURCHASING

Christopher Hughes
Christopher Hughes (Jun 27, 2019)
Director, Division of Purchasing

Jun 27, 2019
Date

Note: Negotiations on sections 7, 8, 9, 12, 13, 22, 26, & 31.

Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and affiliates who are providing the services agreed to under the

---

[1] **A Sample Participating Addendum will be published after the contracts have been awarded.**
[2] **The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.**

Master Agreement.

Data means all information, whether in oral or written (including electronic) form, created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual or reasonably suspected non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, or integrity of the Non-Public Data or Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

Data Categorization means the process of risk assessment of Data. See also “High Risk Data”, “Moderate Risk Data” and “Low Risk Data”.

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity’s’ software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Services under this Master Agreement and billing Customers directly for such Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems (“High Impact Data”).

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The

consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Moderate Impact Data").

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Non-Public Data means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate. Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person.

Platform as a Service (PaaS) as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Product means any deliverable under this Master Agreement, including Services, software, and any incidental tangible goods.

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement

and becomes financially committed to the purchase.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means the possible or actual unauthorized access to a Purchasing Entity's Non-Public Data and Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (SaaS) as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

3. Term of the Master Agreement: Unless otherwise specified as a shorter term in a Participating Addendum, the term of the Master Agreement will run from contract execution to September 15, 2026.

4. Amendments: The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the Lead State and Contractor.

5. Assignment/Subcontracts: Contractor shall not assign, sell, transfer, or sublet rights, or delegate responsibilities under this Master Agreement, in whole or in part, without the prior written approval of the Lead State.

The Lead State reserves the right to assign any rights or duties, including written assignment of contract administration duties to the NASPO Cooperative Purchasing Organization LLC, doing business as NASPO ValuePoint.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement and an amendment is not necessary.

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its participation upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum. Termination may be in whole or in part. Any termination under this provision shall not affect the rights and obligations attending orders outstanding at the time of termination, including any right of any Purchasing Entity to indemnification by the Contractor, rights of payment for Services delivered and accepted, data ownership, Contractor obligations regarding Purchasing Entity Data, rights attending default in performance an applicable Service Level of Agreement in association with any Order, Contractor obligations under Termination and Suspension of Service, and any responsibilities arising out of a Security Incident or Data Breach The Purchasing Entity shall be liable for charges for work that was performed prior to receipt of the termination notice. In addition, this Contract may be terminated, for Cause by either party, in advance of the specified termination date, upon written notice given to the other party. The party in violation will be given thirty (30) calendar days after notification to correct the violations.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to

those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information. Contractor will not be deemed to have accessed, received, or be in the possession of Confidential Information solely by virtue of the fact that the applicable Purchasing Entity transmits, receives, accesses or stores such information through its use of Contractor's services.

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement , including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity. Such prior written approval shall not be unreasonably withheld.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

10. Defaults and Remedies

a. The occurrence of any of the following events shall be an event of default under this Master Agreement:

(1) Nonperformance of contractual requirements; or

(2) A material breach of any term or condition of this Master Agreement; or

(3) Any certification, representation or warranty by Contractor in response to the solicitation or in this Master Agreement that proves to be untrue or materially misleading; or

(4) Institution of proceedings under any bankruptcy, insolvency, reorganization or similar law, by or against Contractor, or the appointment of a receiver or similar officer for Contractor or any of its property, which is not vacated or fully stayed within thirty (30) calendar days after the institution or occurrence thereof; or

(5) Any default specified in another section of this Master Agreement.

b. Upon the occurrence of an event of default, Lead State shall issue a written notice of default, identifying the nature of the default, and providing a period of 30 calendar days in which Contractor shall have an opportunity to cure the default. The Lead State shall not be required to provide advance written notice or a cure period and may immediately terminate this Master Agreement in whole or in part if the Lead State, in its sole discretion, determines that it is reasonably necessary to preserve public safety or prevent immediate public crisis. Time allowed for cure shall not diminish or eliminate Contractor's liability for damages.

c. If Contractor is afforded an opportunity to cure and fails to cure the default within the period specified in the written notice of default, Contractor shall be in breach of its obligations under this Master Agreement and Lead State shall have the right to exercise

any or all of the following remedies:

(1) Exercise any remedy provided by law; and

(2) Terminate this Master Agreement and any related Contracts or portions thereof; and

(3) Suspend Contractor from being able to respond to future bid solicitations; and

(4) Suspend Contractor's performance; and

(5) Withhold payment until the default is remedied.

d. Unless otherwise specified in the Participating Addendum, in the event of a default under a Participating Addendum, a Participating Entity shall provide a written notice of default as described in this section and have all of the rights and remedies under this paragraph regarding its participation in the Master Agreement, in addition to those set forth in its Participating Addendum. Nothing in these Master Agreement Terms and Conditions shall be construed to limit the rights and remedies available to a Purchasing Entity under the applicable commercial code.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

12. Force Majeure: Neither party shall be in default by reason of any failure in performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, acts of the government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party. Nothing herein limits or reduces the Purchasing Entity's payment obligations for past or ongoing Services rendered by Contractor; provided, however, that Contractor acknowledges that such an event may permissibly delay such payment for a period not to exceed sixty (60) business days, if such event directly impacts the Purchasing Entity's payment facilities.

13. Indemnification

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, injury, or damage to property arising directly or indirectly from act(s), error(s), or omission(s) of the Contractor, its employees

or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to any claims arising from the combination of the Product with any other product, system or method, unless the Product, system or method is:

(a) provided by the Contractor or the Contractor's subsidiaries or affiliates;

(b) specified by the Contractor to work with the Product; or

(c) reasonably required, in order to use the Product in its intended manner, and the infringement could not have been avoided by substituting another reasonably available product, system or method capable of performing the same function; or

(d) It would be reasonably expected to use the Product in combination with such product, system or method.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. To the extent and indemnification obligation of Contractor applies under this Section 13.b, and if the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

THIS SECTION 13.B. STATES THE ENTIRE OBLIGATION OF CONTRACTOR AND ITS SUPPLIERS, AND THE EXCLUSIVE REMEDY OF THE INDEMNIFIED PARTIES, IN RESPECT OF ANY INFRINGEMENT OR ALLEGED INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OR PROPRIETARY RIGHTS. THIS INDEMNITY OBLIGATION AND REMEDY ARE GIVEN TO THE INDEMNIFIED PARTIES SOLELY FOR THEIR BENEFIT AND IN LIEU OF, AND CONTRACTOR DISCLAIMS ALL WARRANTIES, CONDITIONS, AND OTHER TERMS OF NONINFRINGEMENT WITH RESPECT TO ANY PRODUCT.

c. Limitation of Liability. Except as otherwise set forth in the Indemnification section above, the limit of liability shall be as follows:

i. Contractor's liability for any claim, loss or liability arising out of, or connected with the Services provided, and whether based upon default, or other liability such as breach of contract, warranty, negligence, misrepresentation or otherwise, shall in no case exceed direct damages in: (i) an amount equal to two (2) times the charges specified in the Purchase Order for the Services, or parts thereof forming the basis of the Purchasing Entity's claim, (said amount not to exceed a total of twelve (12) months charges payable under the applicable Purchase Order) or (ii) five million dollars ($5,000,000), whichever is greater.

ii. The Purchasing Entity may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Purchasing Entity unless Contractor at the time of the presentation of claim shall demonstrate to the Purchasing Entity's satisfaction that sufficient monies are set aside by the Contractor in the form of a bond or through insurance coverage to cover associated damages and other costs.

iii. Notwithstanding the above, neither the Contractor nor the Purchasing Entity shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Purchasing Entity, the Contractor, or by others.

iv. The limitations of liability in this section will not apply to claims for bodily injury or death as set forth in Section 13, and Section 31 – Data Privacy.

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum.

15. Individual Customers: Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for their purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for their purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible for each of the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$3 million general aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage
Low Risk Data	$2,000,000

Moderate Risk Data	$5,000,000
High Risk Data	$10,000,000

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

(4) Professional Liability. As applicable, Professional Liability Insurance Policy in the minimum amount of $1,000,000 per occurrence and $1,000,000 in the aggregate, written on an occurrence form that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every

insurance requirement specified in this section. Failure to provide evidence of coverage may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

18. No Waiver of Sovereign Immunity: In no event shall this Master Agreement, any Participating Addendum or any contract or any Purchase Order issued thereunder, or any act of a Lead State, a Participating Entity, or a Purchasing Entity be a waiver of any form of defense or immunity, whether sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States or otherwise, from any claim or from the jurisdiction of any court.

This section applies to a claim brought against the Participating State only to the extent Congress has appropriately abrogated the Participating State's sovereign immunity and is not consent by the Participating State to be sued in federal court. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

19. Ordering

a. Master Agreement order and purchase order numbers shall be clearly shown on all acknowledgments, shipping labels, packing slips, invoices, and on all correspondence.

b. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms having a Master Agreement on an "as needed" basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. Contractor is expected to become familiar with the Purchasing Entities' rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

d. Contractor shall not begin providing Services without a valid Service Level Agreement or other appropriate commitment document compliant with the law of the Purchasing Entity.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

(1) The services or supplies being delivered;
(2) The place and requested time of delivery;
(3) A billing address;
(4) The name, phone number, and address of the Purchasing Entity representative;
(5) The price per unit or other pricing elements consistent with this Master Agreement and the contractor's proposal;
(6) A ceiling amount of the order for services being ordered; and
(7) The Master Agreement identifier and the Participating State contract identifier.

g. All communications concerning administration of Orders placed shall be furnished solely to the authorized purchasing agent within the Purchasing Entity's purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement. Contractor is reminded that financial obligations of Purchasing Entities payable after the current applicable fiscal year are contingent upon agency funds for that purpose being appropriated, budgeted, and otherwise made available.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform in accordance with the terms of any Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders placed after the expiration or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or

constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office[3].

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. States or other entities permitted to participate may use an informal competitive process to determine which Master Agreements to participate in through execution of a Participating Addendum. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to

---

[3] Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; sales of goods to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this subsection must be consistent with license rights granted for use of intellectual property.

21. Payment: Orders under this Master Agreement are fixed-price or fixed-rate orders, not cost reimbursement contracts. Unless otherwise stipulated in the Participating Addendum, Payment is normally made within 30 days following the date of a correct invoice is received. Purchasing Entities reserve the right to withhold payment of a portion (including all if applicable) of disputed amount of an invoice. After 45 days the Contractor may assess overdue account charges up to a maximum rate of one percent per month on the outstanding balance. Payments will be remitted by mail. Payments may be made via a State or political subdivision "Purchasing Card" with no additional charge.

22. Data Access Controls: In connection with providing the SaaS Services, Contractor may have access to Purchasing Entity's Data. Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on the course of data center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may not share a Purchasing Entity's Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Purchasing Entity Data: Purchasing Entity retains full right and title to Data provided by it and any Data derived therefrom, including metadata.
Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. The obligation shall extend beyond the term of this Master Agreement in perpetuity.

Contractor shall not use any information collected in connection with this Master Agreement, including Purchasing Entity Data, for any purpose other than fulfilling its obligations under this Master Agreement.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, once a year and at no cost to the Contractor and with a thirty (3) day prior written notice to audit, inspect, examine, copy and/or transcribe copies of Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement and applicable Participating Addendum terms. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing

entity's expense.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

30. Data Privacy: The Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. Prior to entering into a SLA with a Purchasing Entity, the Contractor and Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

31. Warranty: At a minimum the Contractor must warrant the following:

a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.

b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation are true and accurate in all material respects.

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the Services it acquires from this Master Agreement.

e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.

f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, ALL SERVICES AND PRODUCTS ARE PROVIDED "AS IS." CONTRACTOR DISCLAIMS ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. CONTRACTOR MAKES NO WARRANTIES OR REPRESENTATIONS THAT ANY SERVICE WILL BE FREE FROM LOSS OR LIABILITY ARISING OUT OF HACKING OR SIMILAR MALICIOUS ACTIVITY, OR ANY ACT OR OMISSION OF THE CUSTOMER.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at no additional cost to the Purchasing Entity. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as required by the Purchasing Entity.

33. Waiver of Breach: Failure of the Lead State, Participating Entity, or Purchasing Entity to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or Participating Addendum. Any waiver by the

Lead State, Participating Entity, or Purchasing Entity must be in writing. Waiver by the Lead State or Participating Entity of any default, right or remedy under this Master Agreement or Participating Addendum, or by Purchasing Entity with respect to any Purchase Order, or breach of any terms or requirements of this Master Agreement, a Participating Addendum, or Purchase Order shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, Participating Addendum, or Purchase Order.

34. Assignment of Antitrust Rights: Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

36. Performance and Payment Time Frames that Exceed Contract Duration: All maintenance or other agreements for services entered into during the duration of an SLA and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No new leases, maintenance or other agreements for services may be executed after the Master Agreement has expired. For the purposes of this section, renewals of maintenance, subscriptions, SaaS subscriptions and agreements, and other service agreements, shall not be considered as "new."

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with JAGGAER, formerly SciQuest, whereby JAGGAER will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II

to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

41. Government Support: No support, facility space, materials, special access, personnel or other obligations on behalf of the states or other Participating Entities, other than payment, are required under the Master Agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://calculator.naspovaluepoint.org. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment H.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical

identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data within the Participating State.

43. NASPO ValuePoint Cooperative Program Marketing, Training, and Performance Review:

a. Contractor agrees to work cooperatively with NASPO ValuePoint personnel. Contractor agrees to present plans to NASPO ValuePoint for the education of Contractor's contract administrator(s) and sales/marketing workforce regarding the Master Agreement contract, including the competitive nature of NASPO ValuePoint procurements, the Master agreement and participating addendum process, and the manner in which qualifying entities can participate in the Master Agreement.

b. Contractor agrees, as Participating Addendums become executed, if requested by ValuePoint personnel to provide plans to launch the program within the participating state. Plans will include time frames to launch the agreement and confirmation that the Contractor's website has been updated to properly reflect the contract offer as available in the participating state.

c. Contractor agrees, absent anything to the contrary outlined in a Participating Addendum, to consider customer proposed terms and conditions, as deemed important to the customer, for possible inclusion into the customer agreement. Contractor will ensure that their sales force is aware of this contracting option.

d. Contractor agrees to participate in an annual contract performance review at a location selected by the Lead State and NASPO ValuePoint, which may include a discussion of marketing action plans, target strategies, marketing materials, as well as Contractor reporting and timeliness of payment of administration fees.

e. Contractor acknowledges that the NASPO ValuePoint logos may not be used by Contractor in sales and marketing until a logo use agreement is executed with NASPO ValuePoint.

f. The Lead State expects to evaluate the utilization of the Master Agreement at the annual performance review. Lead State may, in its discretion, terminate the Master Agreement pursuant to section 6 when Contractor utilization does not warrant further administration of the Master Agreement. The Lead State may exercise its right to not renew the Master Agreement if vendor fails to record or report revenue for three consecutive quarters, upon 60-calendar day written notice to the Contractor. This subsection does not limit the discretionary right of either the Lead State or Contractor to terminate the Master Agreement pursuant to section 7.

g. Contractor agrees, within 30 days of their effective date, to notify the Lead State and NASPO ValuePoint of any contractual most-favored-customer provisions in third-part contracts or agreements that may affect the promotion of this Master Agreements or whose terms provide for adjustments to future rates or pricing based on rates, pricing in, or Orders from this master agreement. Upon request of the Lead State or NASPO ValuePoint, Contractor shall provide a copy of any such provisions.

45. NASPO ValuePoint Cloud Offerings Search Tool: In support of the Cloud Offerings Search Tool here: http://www.naspovaluepoint.org/#/contract-details/71/search Contractor shall ensure its Cloud Offerings are accurately reported and updated to the Lead State in the format/template shown in Attachment I.

46. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. No click-through, or other end user terms and conditions or agreements required by the Contractor ("Additional Terms") provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.

Exhibit 1 to the Master Agreement: Software-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification:

a. Incident Response: Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.

b. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Personal Data Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a Data Breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a data breach is a direct result of Contractor's breach of its contractual obligation to encrypt personal data or otherwise prevent its release as reasonably determined by the Purchasing Entity, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract it's data and the subsequent secure disposal of purchasing entity's data.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

- 10 days after the effective date of termination, if the termination is in accordance with the contract period
- 30 days after the effective date of termination, if the termination is for convenience
- 60 days after the effective date of termination, if the termination is for cause

After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks: Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports: The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Right to Remove Individuals: The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately remove such individual. The Contractor shall not assign the

person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

19. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

22. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

23. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 2 to the Master Agreement: Platform-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

a. Incident Response: The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Master Agreement, Participating Addendum, or SLA. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed, defined by law or contained in the Master Agreement, Participating Addendum, or SLA.

b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall immediately report a security incident related to its service under the Master Agreement, Participating Addendum, or SLA to the appropriate Purchasing Entity.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Purchasing Entity data that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity within 24 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably

requested by the Purchasing Entity to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA and agreed to by both the Contractor and the Purchasing Entity. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or SLA.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 or any other state laws or administrative regulations identified by the Participating Entity..

20. Web Services: The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

21. Encryption of Data at Rest: The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

22. Subscription Terms: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for PaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 3 to the Master Agreement: Infrastructure-as-a-Service

1. Data Ownership: The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. Data Location: The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. Security Incident or Data Breach Notification: The Contractor shall inform the Purchasing Entity of any security incident or data breach related to Purchasing Entity's Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

a. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

b. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA.

a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

c. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state (or federal) law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $217 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

6. Notification of Legal Requests: The Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted

and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. Background Checks:

a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. Access to Security Logs and Reports:

a. The Contractor shall provide reports on a schedule specified in the SLA to the Contractor directly related to the infrastructure that the Contractor controls upon which the Purchasing Entity's account resides. Unless otherwise agreed to in the SLA, the Contractor shall provide the public jurisdiction a history or all API calls for the Purchasing Entity account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Contractor. The report will be sufficient to enable the Purchasing Entity to perform security analysis, resource change tracking and compliance auditing

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. Contract Audit: The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually and at its own expense, and provide an unredacted version of the audit report upon request. The Contractor may remove its proprietary information from the unredacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.

12. Change Control and Advance Notice: The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. Security: As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Import and Export of Data: The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. Responsibilities and Uptime Guarantee: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. Subcontractor Disclosure: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. **Subscription Terms:** Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for IaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Attachment B – Scope of Services Awarded to Contractor

1.1 Awarded Service Model(s).

Contractor is awarded the following Service Model:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

1.2 Risk Categorization.*

Contractor's offered solutions offer the ability to store and secure data under the following risk categories:

Service Model	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered
IaaS	X	X	X	Public /Hybrid / Private
PaaS	X	X	X	Public / Hybrid / Private
SaaS	X	X	X	Public/ Hybrid/ Private

*Contractor may add additional OEM solutions during the life of the contract.

2.1 Deployment Models.

Contractor may provide cloud based services through the following deployment methods:

- **Private cloud.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
- **Community cloud.** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
- **Public cloud.** The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
- **Hybrid cloud.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Attachment C - Pricing Discounts and Schedule

Contractor: Red River Technology LLC

Pricing Notes

1. % discounts are based on minimum discounts off Contractor's commercially published pricelists versus fixed pricing. Nonetheless, Orders will be fixed-price or fixed-rate and not cost reimbursable contracts. Contractor has the ability to update and refresh its respective price catalog, as long as the agreed-upon discounts are fixed.

2. Minimum guaranteed contract discounts do not preclude an Offeror and/or its authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.

3. Purchasing entities shall benefit from any promotional pricing offered by Contractor to similar customers. Promotional pricing shall not be cause for a permanent price change.

4. Contractor's price catalog include the price structures of the cloud service models, value added services (i.e., Maintenance Services, Professional Services, Etc.), and deployment models that it intends to provide including the types of data it is able to hold under each model. Pricing shall all-inclusive of infrastructure and software costs and management of infrastructure, network, OS, and software.

5. Contractor provides tiered pricing to accompany its named user licensing model, therefore, as user count reaches tier thresholds, unit price decreases.

Cloud Service Model: Infrastructure as a Service (IaaS)

Description	Minimum Discount % Off
AWS	3.00%
Average IaaS OEM Discount Off	**3.00%**

Cloud Service Model: Platform as a Service (PaaS)

Description	Discount
AWS	3.00%
Average PaaS OEM Discount Off	**3.00%**

Cloud Service Model: Software as a Service (SaaS)

Description	Discount
AppDynamics	13.00%
AWS	3.00%
ServiceNow	3.50%
Average SaaS OEM Discount Off	**6.50%**

Additional Value Added Services

		Onsite Hourly Rate		Remote Hourly Rate	
Item Description		**NVP Price**	**Catalog Price**	**NVP Price**	**Catalog Price**
Maintenance Services		N/A	N/A	N/A	N/A
Professional Services		N/A	N/A	N/A	N/A
	Deployment Services	N/A	N/A	N/A	N/A
	Integration Services)	N/A	N/A	N/A	N/A
	Consulting/Advisory Services	N/A	N/A	N/A	N/A
	Architectural Design Services	N/A	N/A	N/A	N/A
	Statement of Work Services	N/A	N/A	N/A	N/A
Partner Services		N/A	N/A	N/A	N/A
Training Deployment Services		N/A	N/A	N/A	N/A
Cloud Staffing Roles (Red River Technical Response: Value-Added Services)		N/A	N/A	N/A	N/A
	Cloud Strategist	$291.55	$343.00	$291.55	$343.00
	Cloud Enterprise Architect	$291.55	$343.00	$291.55	$343.00
	Cloud Managed Services Architect	$291.55	$343.00	$291.55	$343.00
	Senior Cloud Program Manager	$291.55	$343.00	$291.55	$343.00
	Cloud Program Manager	$232.05	$273.00	$232.05	$273.00
	Senior Cloud Subject Matter Expert	$267.75	$315.00	$267.75	$315.00
	Cloud Subject Matter Expert	$226.10	$266.00	$226.10	$266.00
	Senior Cloud Configuration and Development Specialist	$220.15	$259.00	$220.15	$259.00
	Cloud Configuration and Development Specialist	$184.45	$217.00	$184.45	$217.00
	Senior Cloud Network Specialist	$220.15	$259.00	$220.15	$259.00
	Cloud Network Specialist	$184.45	$217.00	$184.45	$217.00
	Senior Cloud Security Specialist	$267.75	$315.00	$267.75	$315.00
	Cloud Security Specialist	$214.20	$252.00	$214.20	$252.00
	Senior Cloud Analyst	$208.25	$245.00	$208.25	$245.00
	Cloud Analyst	$160.65	$189.00	$160.65	$189.00
	Senior Cloud Operations Lead	$208.25	$245.00	$208.25	$245.00
	Cloud Operations Lead	$160.65	$189.00	$160.65	$189.00
	Senior Cloud Operations Analyst	$178.50	$210.00	$178.50	$210.00
	Cloud Operations Analyst	$148.75	$175.00	$148.75	$175.00

	Deliverable Rates	
	NVP Price	**Catalog Price**
N/A	N/A	N/A

Red River Technical Response

The State of Utah
NASPO ValuePoint Master Agreement for Cloud Solutions
Solicitation No. SK18008
July 6, 2018

Red River's response to the items described in Section 8 of the RFP

RED RIVER TECHNOLOGY LLC
21 WATER STREET, SUITE 500
CLAREMONT, NH 03743
603 448 8880
www.redriver.com

DUNS #: 933678708
CAGE CODE: 04MB1
TIN #: 02-0483341

Submitted By:
Dan McGee
COO, Red River Technology LLC
Red River Technology LLC
+1-603-442-5513, dan.mcgee@redriver.com

Submitted to:
Solomon Kingston, State Contract Analyst
State of Utah, Division of Purchasing
skingston@utah.gov
(801) 538-3228

Electronically via SciQuest (the Utah Public Procurement Place) here:
http://bids.sciquest.com/apps/Router/PublicEvent?CustomerOrg=StateOfUtah

This proposal includes information that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate this proposal or quotation. If, however, a contract is awarded to a result of or in connection with the submission of this information, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this proposal or quotation if it is obtained from another source without restriction. The information subject to this restriction is contained on sheets with the following disclosure legend: "Use or disclosure of information contained on this sheet is subject to the restriction on the title page of this proposal."

Table of Contents

TECHNICAL RESPONSE: NARRATIVE (RESPONSE TO RFP 3.10.6.A) 1

TECHNICAL RESPONSE: POINT-BY-POINT (RESPONSE TO RFP 3.10.6.B) 1

1. (M)(E) TECHNICAL REQUIREMENTS.....2

1.1 NIST Special Publication 800-145 (8.1.1) 2
1.1.1 AppDynamics 2
1.1.2 Amazon Web Services (AWS)..... 2
1.1.3 ServiceNow 3
1.2 Compliance with Attachment C NIST Service Models & Attachment D Scope of Services (8.1.2)..... 5
1.3 Adherence to Attachment D Scope of Services (8.1.3)..... 5

2. (E) SUBCONTRACTORS 7

2.1 Use of Contractors (8.2.1)..... 7
2.1.1 AppDynamics 7
2.1.2 AWS..... 7
2.1.3 ServiceNow 7
2.2 Extent of Use of Subcontractors (8.2.2)..... 8
2.3 Qualifications of Subcontractors (8.2.3)..... 9

3. (E) WORKING WITH PURCHASING ENTITIES 11

3.1 Data Breach (8.3.1)..... 11
3.1.1 AppDynamics 12
3.1.2 AWS..... 12
3.1.3 ServiceNow 13
3.2 Adware, Software or Marketing (8.3.2) 15
3.3 User Test/Staging Environment (8.3.3) 15
3.3.1 AppDynamics 15
3.3.2 AWS..... 15
3.3.3 ServiceNow 15
3.4 Access for People with Disabilities (8.3.4)..... 15
3.4.1 AppDynamics 16
3.4.2 AWS..... 16
3.4.3 ServiceNow 16
3.5 Applications and Web Browsers (8.3.5) 16
3.5.1 AppDynamics 16
3.5.2 AWS..... 17
3.5.3 ServiceNow 17

Table of Contents

3.6 Service Level Agreements (8.3.6) 18
3.6.1 AppDynamics 18
3.6.2 AWS 18
3.6.3 ServiceNow 19
3.7 Project Schedules/Work Plans (8.3.7) 20
3.7.1 Project/Program Management Library 20
3.7.2 Project Schedule View 21
3.7.3 Executive Roadmaps 22
3.8 Technology Changes (8.3.7) 24
3.8.1 AppDynamics 25
3.8.2 AWS 26
3.8.3 ServiceNow 26

4. (E) CUSTOMER SERVICE (8.4) 27

4.1 Excellent Customer Service (8.4.1) 27
4.1.1 AppDynamics 28
4.1.2 AWS 28
4.1.3 ServiceNow 31
4.2 Complying with Customer Service Requirements (8.4.2) 31
4.2.1 AppDynamics 32
4.2.2 AWS 32
4.2.3 ServiceNow 33

5. (E) SECURITY OF INFORMATION (8.5) 34

5.1 Protecting Data (8.5.1) 34
5.1.1 AppDynamics 34
5.1.2 AWS 34
5.1.3 ServiceNow 35
5.2 Complying with Applicable Laws (8.5.2) 36
5.2.1 AppDynamics 37
5.2.2 AWS 37
5.2.3 ServiceNow 38
5.3 Access to a Purchasing Entity's Accounts (8.5.3) 38
5.3.1 AppDynamics 38
5.3.2 AWS 39
5.3.3 ServiceNow 39

6. (E) PRIVACY AND SECURITY (8.6) 40

6.1 Compliance with Industry Standards (8.6.1) 40
6.1.1 AppDynamics 40
6.1.2 AWS 40
6.1.3 ServiceNow 40
6.2 Security Certifications (8.6.2) 41

Table of Contents

6.2.1 AppDynamics 42
6.2.2 AWS 42
6.2.3 ServiceNow 42
6.3 Security Practices (8.6.3) 43
6.3.1 AppDynamics 43
6.3.2 AWS 43
6.3.3 ServiceNow 45
6.4 Data Confidentiality Standards (8.6.4) 46
6.4.1 AppDynamics 46
6.4.2 AWS 46
6.4.3 ServiceNow 47
6.5 Third-Party Certifications (8.6.5) 47
6.5.1 AppDynamics 47
6.5.2 AWS 48
6.5.3 ServiceNow 48
6.6 Logging Process (8.6.6) 48
6.6.1 AppDynamics 48
6.6.2 AWS 48
6.6.3 ServiceNow 51
6.7 Restrict Visibility (8.6.7) 51
6.7.1 AppDynamics 52
6.7.2 AWS 52
6.7.3 ServiceNow 53
6.8 Notification Process (8.6.8) 53
6.8.1 AppDynamics 53
6.8.2 AWS 53
6.8.3 ServiceNow 53
6.9 Security Controls (8.6.9) 54
6.9.1 AppDynamics 54
6.9.2 AWS 54
6.9.3 ServiceNow 55
6.10 Security Technical Reference Architectures (8.6.10) 56
6.10.1 AppDynamics 56
6.10.2 AWS 56
6.10.3 ServiceNow 56
6.11 Employee Security Procedures (8.6.11) 58
6.11.1 AppDynamics 59
6.11.2 AWS 59
6.11.3 ServiceNow 60
6.12 Confidentiality of Data Types (8.6.12) 60
6.12.1 AppDynamics 60
6.12.2 AWS 60
6.12.3 ServiceNow 61
6.13 Data Breach Notification (8.6.13) 61
6.13.1 AppDynamics 62
6.13.2 AWS 62

Table of Contents

6.13.3 ServiceNow 62

7. (E) MIGRATION AND REDEPLOYMENT PLAN (8.7) 64

7.1 Closing Down a Service (8.7.1) 64
7.1.1 AppDynamics 64
7.1.2 AWS 64
7.1.3 ServiceNow 65
7.2 Return of Data (8.7.2) 65
7.2.1 AppDynamics 65
7.2.2 AWS 65
7.2.3 ServiceNow 66

8. (E) SERVICE OR DATA RECOVERY (8.8) 67

8.1 Service or Data Recovery Steps (8.8.1) 67
8.1.1 AppDynamics 67
8.1.2 AWS 68
8.1.3 ServiceNow 70
8.2 Backup and Restore Services (8.8.2) 71
8.2.1 AppDynamics 72
8.2.2 AWS 72
8.2.3 ServiceNow 72

9. (E) DATA PROTECTION (8.9) 73

9.1 Protecting Data (8.9.1) 73
9.1.1 AppDynamics 73
9.1.2 AWS 73
9.1.3 ServiceNow 74
9.2 Business Associate Agreement (8.9.2) 74
9.2.1 AppDynamics 74
9.2.2 AWS 75
9.2.3 ServiceNow 75
9.3 Use of Data (8.9.3) 75
9.3.1 AppDynamics 75
9.3.2 AWS 76
9.3.3 ServiceNow 76

10. (E) SERVICE LEVEL AGREEMENTS (8.10) 77

10.1 Service Level Agreement Negotiations (8.10.1) 77
10.1.1 AppDynamics 77
10.1.2 AWS 77
10.1.3 ServiceNow 78
10.2 Service Level Agreement Sample (8.10.2) 78

Table of Contents

10.2.1 AppDynamics 78
10.2.2 AWS 79
10.2.3 ServiceNow 79

11. (E) DATA DISPOSAL (8.11) 80

11.1 Data Disposal Procedures (8.11.1) 80
11.1.1 AppDynamics 80
11.1.2 AWS 80
11.1.3 ServiceNow 80

12. (E) PERFORMANCE MEASURES AND REPORTING (8.12) 82

12.1 Reliability and Uptime (8.12.1) 82
12.1.1 AppDynamics 82
12.1.2 AWS 82
12.1.3 ServiceNow 83
12.2 Uptime (8.12.1) 83
12.2.1 AppDynamics 83
12.2.2 AWS 84
12.2.3 ServiceNow 84
12.3 Support (8.12.3) 84
12.3.1 AppDynamics 84
12.3.2 AWS 85
12.3.3 ServiceNow 85
12.4 SLA Remedies (8.12.4) 85
12.4.1 AppDynamics 86
12.4.2 AWS 86
12.4.3 ServiceNow 86
12.5 Downtime (8.12.5) 86
12.5.1 AppDynamics 86
12.5.2 AWS 86
12.5.3 ServiceNow 87
12.6 Recovery Metrics Not Met (8.12.6) 87
12.6.1 AppDynamics 87
12.6.2 AWS 88
12.6.3 ServiceNow 88
12.7 Performance Reports (8.12.7) 88
12.7.1 AppDynamics 88
12.7.2 AWS 90
12.7.3 ServiceNow 90
12.8 Printing Reports (8.12.8) 91
12.8.1 AppDynamics 91
12.8.2 AWS 91
12.8.3 ServiceNow 91
12.9 Support 24x365 (8.12.9) 91

Table of Contents

12.9.1 AppDynamics 91
12.9.2 AWS 91
12.9.3 ServiceNow 93
12.10 Scale-up/down (8.12.10) 94
12.10.1 AppDynamics 94
12.10.2 AWS 94
12.10.3 ServiceNow 94

13. (E) CLOUD SECURITY ALLIANCE (8.13) 95
13.1 CSA Star Registry (8.13.1) 95
13.1.1 AppDynamics 95
13.1.2 AWS 95
13.1.3 ServiceNow 96

14. (E) SERVICE PROVISIONING (8.14) 97
14.1 Emergency or Rush Services (8.14.1) 97
14.1.1 AppDynamics 97
14.1.2 AWS 97
14.1.3 ServiceNow 97
14.2 Lead-Time for Provisioning (8.14.2) 97
14.2.1 AppDynamics 98
14.2.2 AWS 98
14.2.3 ServiceNow 98

15. (E) BACK UP AND DISASTER PLAN (8.15) 99
15.1 Retention Periods (8.15.1) 99
15.1.1 AppDynamics 99
15.1.2 AWS 99
15.1.3 ServiceNow 99
15.2 Risks and Mitigations (8.15.2) 99
15.2.1 AppDynamics 101
15.2.2 AWS 101
15.2.3 ServiceNow 101
15.3 Data Center Infrastructure (8.15.3) 102
15.3.1 AppDynamics 102
15.3.2 AWS 102
15.3.3 ServiceNow 103
15.4 Documentation (8.16.1) 104
15.4.1 AppDynamics 105
15.4.2 AWS 105
15.4.3 ServiceNow 105
15.5 Tool Sets (8.16.2) 106
15.5.1 AppDynamics 106

Table of Contents

15.5.2 AWS 107
15.5.3 ServiceNow 110

16. (8.17) (E) TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE) 111

16.1 Testing and Training Periods (8.17.1) 111
16.1.1 AppDynamics 111
16.1.2 AWS 111
16.1.3 ServiceNow 111
16.2 Testing and Training Periods (8.17.2) 111
16.2.1 AppDynamics 112
16.2.2 AWS 112
16.2.3 ServiceNow-Validate SN 112
16.3 Training and Support (8.17.3) 112
16.3.1 AppDynamics 112
16.3.2 AWS 112
16.3.3 ServiceNow 113

17. (E) INTEGRATION AND CUSTOMIZATION (8.18) 114

17.1 Integration (8.18.1) 114
17.1.1 AppDynamics 114
17.1.2 AWS 118
17.1.3 ServiceNow 120
17.2 Customization and Personalization (8.18.2) 120
17.2.1 AppDynamics 121
17.2.2 AWS 121
17.2.3 ServiceNow – Validate 122

18. (E) MARKETING PLAN (8.19) 123

18.1 Marketing Solutions (8.19.1) 123
18.1.1 Develop the Message 123
18.1.2 Sales Enablement 124
18.1.3 Nurture Opportunities and Capabilities 125
18.1.4 Demand Generation and Follow-up 126

19. (8.20) (E) RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS 128

19.1 Value-Added Services (8.20.1) 128
19.1.1 Cloud Value-Added Services Framework 128
19.1.2 Cloud Value-Added Staffing Expertise 132

20. (E) SUPPORTING INFRASTRUCTURE (8.22) 138

Table of Contents

20.1 Infrastructure Description (8.22.1) 138
20.1.1 AppDynamics 138
20.1.2 AWS 138
20.1.3 ServiceNow 139
20.2 New Infrastructure Installation (8.22.2) 139
20.2.1 AppDynamics 139
20.2.2 AWS 140
20.2.3 ServiceNow 140

21. APPENDIX: APPDYNAMICS SLA (AS OF 6-29-2018) 141

22. APPENDIX: AMAZON CLOUDFRONT SLA (AS OF 6-29-2018) 158

23. APPENDIX: AMAZON EC2 SLA (AS OF 6-29-2018) 162

24. APPENDIX: AMAZON DYNAMO DB SLA (AS OF 6-29-2018) 167

25. APPENDIX: AMAZON RDS SLA (AS OF 6-29-2018) 172

26. APPENDIX: AMAZON ROUTE 53 SLA (AS OF 6-29-2018) 177

27. APPENDIX: AMAZON S3 SLA (AS OF 6-29-2018) 182

28. APPENDIX: AWS SHIELD ADVANCED SLA (AS OF 6-29-2018) 186

29. APPENDIX: AWS SERVICE DESCRIPTION 189

30. APPENDIX: SERVICENOW SUBSCRIPTION GUIDE-SLA (AS OF 6-29-2018) 217

31. APPENDIX: APPDYNAMICS SECURITY AND PRIVACY STANDARD - CONFIDENTIAL 243

32. APPENDIX: RRMS SLA AND AGREEMENT SAMPLE 249

Table 1: AppDynamics NIST 800-145 Cross-Reference 2
Table 2: AWS NIST 800-145 Cross-Reference 3
Table 3: ServiceNow NIST 800-145 Cross-Reference 5
Table 4: Services, Definitions and Deployment Models 5
Table 5: Key Considerations in Partners and Subcontractors 9

Table of Contents

Table 6: ServiceNow Response Times 14
Table 7: AWS Browser Support 17
Table 8: ServiceNow Browser Support 17
Table 9: Red River Technology Change Strategies 25
Table 10: AWS Customer Support Highlights 30
Table 11: AppDynamics Response Times 32
Table 12: ServiceNow Response Times 33
Table 13: AWS Tools 110
Table 14: AppDynamics Integration Modules 115
Table 15: AppDynamics API Roster 118
Table 16: ServiceNow Integration Highlights 120
Table 17: Sustainment Services Matrix 132
Table 18: Value-Added Cloud Staffing Support 137

Figure 1: Representative Project Schedule 22
Figure 2: Representative Client Roadmap 23
Figure 3: Red River Technology Refresh Approach 24
Figure 4: AWS Isolation and Deployment Options 55
Figure 5: ServiceNow Security Framework 57
Figure 6: ServiceNow Layered Security Model 58
Figure 7: AppDynamics Disaster Process 68
Figure 8: AppDynamics Network Diagram 68
Figure 9: ServiceNow Architecture 71
Figure 10: AppDynamics Virtual War Room 89
Figure 11: AWS Load Balancing 93
Figure 12: AWS Availability Zones 103
Figure 13: Availability Zone 103
Figure 14: High Availability Diagram 104
Figure 15: Red River High-Level Marketing Approach 123
Figure 16: Red River Contract Portfolio Guide and Battlecard 124
Figure 17: Current Cloud-Focused Information and Datasheets 125
Figure 18: Red River Innovation Center 126
Figure 19: Red River Cloud Capability Areas 128
Figure 20: Path to Cloud Value-Added Services 129
Figure 21: Notional Reference Architecture 130
Figure 22: AppDynamics AppServer Agent 138
Figure 23: ServiceNow Architecture 139

TECHNICAL RESPONSE: NARRATIVE (RESPONSE TO RFP 3.10.6.A)

Utah Solicitation Number SK18008 Requirement: Page 14
3.10.6.A. A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offerors ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed.

Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

Red River is pleased to respond to the State of Utah Solicitation No. SK18008 for NASPO ValuePoint Master Agreement for Cloud Solutions. Red River is a cloud solution provider and reseller, providing customers cloud solutions across the nation, from K-12, counties, states and the federal government. We are bidding with our Cloud Solution Providers (CSPs) Amazon Web Services (AWS), ServiceNow and App Dynamics whose offerings are summarized in Table 1. With these three CSPs, Red River can meet all the requirements of this Solicitation.

☑ *Please refer to more granular narrative as part of our point-by-point response in Technical Response: Point-by-Point (Response to RFP 3.10.6.B) below*

TECHNICAL RESPONSE: POINT-BY-POINT (RESPONSE TO RFP 3.10.6.B)

Utah Solicitation Number SK18008 Requirement: Page 14
3.10.6.B. A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP. Offerors should not provide links to a website as part of its response.

Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

Red River has provided a point-by-point response, in the order listed, for each requirement.

1. (M)(E) TECHNICAL REQUIREMENTS

1.1 NIST Special Publication 800-145 (8.1.1)

Utah Solicitation Number SK18008 Requirement: Page 25
8.1.1 For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the characteristics defined in NIST Special Publication 800-145.

The National Institute of Standards and Technology (NIST) definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. The definition is intended to serve as a means for broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing.

1.1.1 AppDynamics

The following table details how AppDynamics meets the NIST definition of cloud.

NIST 800-145 Characteristic	AppDynamics Analysis
On-Demand Self-Service	Yes, AppDynamics complies with this standard. The AppDynamics Platform allows customers to deploy agents in an On-Demand Self-Service capability and point those agents back to the AppDynamics SaaS environment. A license is required for use of the platform
Broad Network Access	Yes, AppDynamics complies with this standard. The AppDynamics User Interface (UI) is accessible through any modern browser or mobile device.
Resource Pooling	Yes, AppDynamics complies with this standard. AppDynamics SaaS is multi-tenant, but can also be served on dedicated systems.
Rapid Elasticity	Yes, AppDynamics complies with this standard. The AppDynamics Platform (specifically the End User Management capability) is dynamically scaled or reduced based on customer demand or load. This elasticity is transparent to the end users of the software.
Measured Service	Yes, AppDynamics complies with this standard. AppDynamics usage is controlled through the use of licenses (number of agents deployed). The UI provides a license usage over time page. Also, through the AppDynamics Portal, customers can view usage patterns (number of logins) of their end users on the service.

Table 1: AppDynamics NIST 800-145 Cross-Reference

1.1.2 Amazon Web Services (AWS)

The following table details how AWS meets the NIST definition of cloud.

NIST 800-145 Characteristic	AWS Analysis
On-Demand Self-Service	AWS provides customers of all sizes with on-demand access to a wide range of cloud infrastructure services, charging you only for the resources you actually use. AWS enables you to eliminate the need for costly hardware and the administrative pain that goes along with owning and operating it. Instead of the weeks and months it takes to plan, budget, procure, set up, deploy, operate, and hire for a new project, our customers can simply sign up for AWS and immediately begin deployment in the cloud with the equivalent of 1, 10, 100, or 1,000 servers. Whether an organization needs to prototype an application or host a production solution, AWS makes it simple for customers to get started and be productive.
Broad Network Access	AWS provides a simple way to access servers, storage, databases, and a broad set of application services over the Internet. Cloud computing providers such as AWS own and maintain the network-connected hardware required for these application services, while you provision and use what you need via a web application.
Resource Pooling	The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, Payment Card Institute (PCI) controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI Data Security Standards (DSS) 3.2 as of July 2016.
Rapid Elasticity	AWS provides a massive global cloud infrastructure that allows you to quickly innovate, experiment, and iterate. Instead of waiting weeks or months for hardware, you can instantly deploy new applications, instantly scale up as your workload grows, and instantly scale down based on demand. Customers need to be confident that their existing infrastructure can handle a spike in traffic and that the spike will not interfere with normal business operations. Elastic Load Balancing and Auto Scaling can automatically scale a customer's AWS resources up to meet unexpected demand and then scale those resources down as demand decreases
Measured Service	AWS uses automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

Table 2: AWS NIST 800-145 Cross-Reference

1.1.3 SERVICENOW

The following table details how ServiceNow meets the NIST definition of cloud.

NIST 800-145 Characteristic	ServiceNow Analysis
On-Demand Self-Service	Yes, ServiceNow complies with this standard. Customer instances are provisioned automatically after an agreement between a customer and ServiceNow is executed. ServiceNow actively monitors customer instance performance and can automatically scale its application servers out horizontally by adding them to the load balancer pools for a particular instance.
Broad Network Access	Yes, ServiceNow complies with this standard. ServiceNow's physical architecture is deployed into ServiceNow's managed dedicated colocation cage space. Multiple diverse Internet connections terminate within the dedicated cage space providing redundant access from the Internet to the ServiceNow environment. All users, administrators and developers connect to the ServiceNow private cloud over Hypertext Transfer Protocol Secure (HTTPS), leveraging Transport Layer Security (TLS), for communication to and from a ServiceNow instance with all normal interactions via a web browser. There is no requirement to install any client software on any desktop, laptop, tablet, or smart phone used to access a ServiceNow instance.
Resource Pooling	Yes, ServiceNow complies with this standard. The ServiceNow environment is a private cloud, fully owned and operated by ServiceNow, which supports a logically single tenant architecture. Customer data is isolated from other customer data by leveraging an enterprise-grade cloud architecture and a dedicated database and application set per instance. This gives ServiceNow customers cost reduction through shared infrastructure, while having the security benefits of customer-specific isolation at the application and data layers. In addition to the security features that come standard within the platform and each customer instance, customers can leverage the additional security features within ServiceNow to augment the security configuration of their instances based on their own needs and risk profile. Customers share a hardware platform (no virtualization), but access entirely separate individual instances of the ServiceNow platform.
Rapid Elasticity	Yes, ServiceNow complies with this standard. ServiceNow is a multi-instance architecture that gives every customer its own unique database, which means that it is impossible for your data to be commingled with any other customer. The multi-instance architecture is not built on large centralized database software and infrastructure. Instead, we deploy instances on a per-customer basis, allowing the multi-instance cloud to scale horizontally and infinitely. For our multi-instance cloud, we deploy separate application logic (Apache Tomcat Java Virtual Machines) and database processes (MySQL) for every customer. This allows ServiceNow to scale its application servers out horizontally by adding them to the load balancer pools for a particular instance.
Measured Service	Yes, ServiceNow complies with this standard. ServiceNow is a subscription service measured by number of user accounts or number of managed nodes. ServiceNow has a documented capacity-planning model, which is used to

NIST 800-145 Characteristic	ServiceNow Analysis
	determine sizing requirements and scaling options. The need to address capacity and horizontal system scaling is in the background, transparent to our customers.

Table 3: ServiceNow NIST 800-145 Cross-Reference

1.2 Compliance with Attachment C NIST Service Models & Attachment D Scope of Services (8.1.2)

Utah Solicitation Number SK18008 Requirement: Page 25
8.1.2 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of Attachments C (NIST Service Models) & D (Scope of Services).

As a responsible contract holder of public sector information technology (IT) contract, Red River is obligated and committed to identifying and representing cloud offerings compliant with the requirements found in Attachments C and D - now and in the future.

1.3 Adherence to Attachment D Scope of Services (8.1.3)

Utah Solicitation Number SK18008 Requirement: Page 25
8.1.3 As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in Attachment D.

Each of the three CSPs proposed have built their offerings to comply with definitions used in the RFP Attachment D Scope of Services, which are in turn derived from FIPS Pub 199 and NIST 800-145. Table 4: Services, Definitions and Deployment Models below demonstrates the services, definitions, and deployment models RFP Attachment D.

CSP	Description	Service Model	Deployment Model	Risk Category
AppDynamics	Cloud-based application performance management and IT operations analytics	• SaaS	• Public • Hybrid • Private	• Low • Moderate
AWS	On-demand cloud computing platforms on a paid subscription basis	• IaaS • PaaS • SaaS	• Public • Hybrid • Private	• Low • Moderate • High
ServiceNow	Cloud-based IT automation services	• SaaS	• Public • Hybrid	• Low • Moderate • High

Table 4: Services, Definitions and Deployment Models

Red River also understands that there will be variances across, or extensions of, the scope of services terms with different states and will collaborate with states to clarify the services, definitions, deployment models and data risk categories in the Participating Addendum.

2. (E) SUBCONTRACTORS

2.1 Use of Contractors (8.2.1)

Utah Solicitation Number SK18008 Requirement: Page 25
8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

Red River has an extensive partner network built around identifying the premier providers – and monitoring performance to verify they remain premier providers. Red River will be utilizing Subcontractors to provide services and solutions for specific manufacturers within this response. Red River will also work with the manufacturers to provide these services and solutions to all Participating Entities. All Subcontractors are, and will continue to be, vetted to verify they have the necessary qualifications to do business within the State of Utah and any applicable Participating States. All Subcontractors will also comply with the applicable terms and conditions of the Request for Proposal (RFP) and subsequent contract, as well as all Participating Addendums.

2.1.1 APPDYNAMICS

Red River will be reselling AppDynamics services and solutions to National Association of State Procurement Officials (NASPO) participating entities. Red River will work with each customer on a case by case basis to determine which is the most cost effective and efficient solution based on their needs. AppDynamics may use sub-contractors and will ensure that any such usage meets the security and other contractual requirements for the service being provided.

2.1.2 AWS

Red River has the flexibility to offer AWS Services directly to the customer or through a certified partner. We will work with each customer on a case by case basis to determine which is the most cost effective and efficient method.

2.1.3 SERVICENOW

Red River will be reselling ServiceNow SaaS solutions to NASPO Participating Entities. Red River will handle all of the logistics for NASPO Entities – scoping, quoting, Purchase Order placement, licensing agreements, usage reports, and billing. Red River is a key partner in the private hosted SaaS solution offering as well as other cloud based offerings.

2.2 Extent of Use of Subcontractors (8.2.2)

Utah Solicitation Number SK18008 Requirement: Page 25
8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.

Red River will be the management point-of-contact on all delivery engagements associated with this NASPO/ValuePoint Master Services Agreement (MSA) and participating Addenda. Red River will use subcontractors as a third-party organization (e.g., corporation, LLC) where there is unique expertise that enhances the quality, speed or cost-effectiveness of the client project.

Red River evaluates potential opportunities to determine if there are Subcontract organizations that can offer unique domain expertise. Table 5: Key Considerations in Partners and Subcontractors identifies key factors we use in identification of value-added Subcontractors.

Delivery Expertise	Red River Analysis
Geography	Our initial strategy is to establish Participating Addenda in states where our geographic footprint is already established and growing, such as: • Northeastern states near our Claremont, NH corporate headquarters and network operating center (NOC) • Mid-Atlantic states near our Reston, VA corporate offices • States bordering the State of Texas where we established an Austin, TX Innovation Center • Western and Northwestern states around our Sacramento, CA Hub of Excellence With our long-standing presence in these areas, we have built and maintain a network of specialists with well-established – and well-proven – capabilities tuned to the local climate, human resources dynamics and other attributes that impact hiring, field management and even items as basic as seasonal travel.
Client Intimacy and Continuity	Red River places importance a detailed understanding of the current client infrastructure and look-forward objectives. Our experience is that there are organizations that have prior successful projects and an acute awareness of the people, process and technology unique to the community. We explore partnering opportunities when there are established organizations with a sterling reputation that can apply their unique knowledge for cost, speed and quality of the engagement. We also have a longstanding history of aligning with partners that, in turn, support varying business enterprise objectives across states, such as small businesses, business located in Hub Zones, service-disabled veteran owned businesses, minority and woman-owned businesses and other important business incentive programs.

Delivery Expertise	Red River Analysis
Implementation Expertise	Red River understands that there is no real substitute for having successfully planned, architected, transitioned and maintained technology engagements. We explore partnering opportunities when other organizations may have "tried and true" resources with the certifications and past performance that can support cost, timeline and quality efficiency.

Table 5: Key Considerations in Partners and Subcontractors

2.3 Qualifications of Subcontractors (8.2.3)

Utah Solicitation Number SK18008 Requirement: Page 25
8.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

Red River will make the determination of the need and value of specific Subcontractor arrangements as appropriate to the final NASPO/ValuePoint MSA and associated Participating Addenda. Our experience indicates that the specific roles and responsibilities will vary as the delivery engagement needs vary – but in all cases - Red River will be responsible for the clear delineation of roles and responsibilities in any delivery engagement. Beyond our qualifications and past performance vetting, we verify and document that any organization has at least the following before adding them as a Subcontractor:

- Certifications in good-standing necessary to do business in the State
- Industry best practices to catalog past criminal activity of the organization or its' principals
- Credit checks and other industry best practices to verify financial stability necessary to achieve the delivery engagement target

We meet directly with any potential Subcontractors on multiple occasions to confirm that they are reliable and exceed expectations as a services and solutions provider. Red River, as Prime Contractor, implements clear, concise subcontracting policies and procedures that define Red River as accountable for NASPO/ValuePoint and Participating Entities contract performance. We understand that developing, negotiating, and executing sound subcontracts sets the proper tone for subcontractor performance. We "flow down" the applicable terms and conditions of the contract as appropriate to the subcontract and establish a clear definition of the area of services to be provided, expectations for performance, identification of key personnel, and establishment of procedures to handle disputes.

All Team members are fully integrated in the project organization and will work alongside Red River staff as an integrated team. Individuals will be assigned responsibilities for specific duties on tasks - but only a single, unified team, dedicated to meeting project objectives, will be visible to Participating Entities. Regardless of which team member accomplishes the work, all

deliverables are the responsibility of Red River. To achieve efficient contract performance, subcontractor management will be an integral function of our management approach, based on the following principles:

- Establish and maintain frequent, open communications and ensure that all subcontractor personnel adhere to the same standards, policies, and procedures as Red River personnel;
- Coordinate resource needs/concerns at the Program Management Office (PMO) level between PM and subcontractor liaisons;
- Convey assignments with a simple, clear SOW with well-defined milestones and deliverables;
- Leverage our internal Red River ServiceNow capability for task assignment, completion notification, and reporting capabilities to provide seamless collaboration across all members of the Team; and
- Periodically monitor our project review process as part of our proposed International Organization for Standardization (ISO)-driven Quality Control (QC) program.

A subcontractor will be actively involved in understanding and shaping any Statements of Work created for the services of a deal in order to make sure that they have the capacity to meet all of the necessary requirements. These Statements of Work will dictate the terms upon which the subcontractor is deployed for services, so Red River will work specifically with subcontractors that are active in the public sector and understand the nuances of selling to government entities.

3. (E) WORKING WITH PURCHASING ENTITIES

3.1 Data Breach (8.3.1)

Utah Solicitation Number SK18008 Requirement: Page 25
8.3.1 Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

- *Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;*
- *Response times;*
- *Processes and timelines;*
- *Methods of communication and assistance; and*
- *Other information vital to understanding the service you provide.*

Red River currently operates a U.S.-based, SOC-2 and ISO 9001:2015 certified NOC where we provide Managed Services capabilities at response thresholds defined collaboratively for a client engagement. Each of the CSPs we have proposed can provide an extensive array of incident management capabilities as outlined below. As described throughout this proposal and notably in Section 19 (E) RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS (8.20) beginning on page 128, Red River can provide direct Managed Services support in addition to the excellent capabilities of each CSP. We highlight these capabilities here as context that Red River understands the end-to-end support model and, at client request, can provide direct support.

The Red River Contract Manager, Phillip Wieser, will be the first to be notified and then will notify the customer – please see Section 8.4.1 Customer Service. Our certified engineers are available 24x7x365 to maintain watch and spring into action when these operations generate abnormalities or incidents outside of pre-established operational guidelines. Red River's NOC uses only best-in-class support tools and working directly with the CSPs and client to facilitate troubleshooting and to follow incidents through to complete resolution.

Red River's Managed Services Focus includes:

- IT Problem Resolution
- 24/7/365 Support
- Issue Escalation (Levels 1, 2 & 3 Support)
- Advanced Technical Support
- Customized Response Procedures
- Back-Up & Recovery Support
- Complete Network Support
- Telephone Infrastructure Support
- Incident Lifecycle Management

3.1.1 AppDynamics

AppDynamics maintains an Incident Response Policy and trains all personnel identified in the policy of their responsibilities on a semi-annual basis. In the event of a suspected incident the incident response team is notified and immediately begins a reasonable investigation as to whether or not a breach has occurred. AppDynamics will also immediately notify the Red River Contract Manager, Phillip Wieser and he will then notify the customer (please see Section 4.1 Excellent Customer Service (8.4.1) on page 27). In the event of a reasonably suspected breach, AppDynamics will use commercially reasonable efforts to contain, mitigate, and resolve the breach as well as put in place additional controls to prevent further breaches of a similar type.

AppDynamics has retained a leading incident response provider to provide additional incident response capabilities and reserves the right to engage their services without prior approval from affected customers.

Where allowed by applicable law, AppDynamics will promptly (not later than 48 hours) notify affected customers of a security incident that affects Customer Data, typically via email provided to AppDynamics by the customer. Once AppDynamics has reasonably determined that Customer Data has been impacted, AppDynamics will promptly notify the impacted customer(s) following such determination. In accordance with its Incident Response Policy, AppDynamics will provide reasonable details regarding the incident, the steps taken by AppDynamics to contain, mitigate, resolve, and prevent future incidents provided that, in AppDynamics' sole discretion, such information does not impact the confidentiality of other AppDynamics customers or the overall security posture of AppDynamics.

AppDynamics, in its sole discretion, may publicly disclose the fact that a security incident has occurred but will not name affected customers. Additionally, in accordance with its Information Security Policy, AppDynamics may notify local, state, federal, and or international law enforcement agencies.

3.1.2 AWS

AWS services are content agnostic, in that they offer the same high level of security to all customers, regardless of the type of content being stored, or the geographical region in which they store their content. Customers retain ownership and control of their content when using AWS services. Customers, rather than AWS, determine what content they store or process using AWS services. Because it is the customer who decides what content to place in the AWS cloud, only the customer can determine what level of security is appropriate for the content they store and process using AWS. Given that customers maintain control of their content when using AWS, customers retain the responsibility to monitor their own environment for privacy breaches and to notify regulators and affected individuals as required under applicable law.

AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment and has been developed in alignment with the ISO 27001 standards, system utilities are appropriately restricted and monitored. Below is an outline of the three-phased approach AWS has implemented to manage incidents:

- Activation and Notification Phase: Incidents for AWS begin with the detection of an event. This can come from several sources including:
    - Metrics and alarms – AWS maintains an exceptional situational awareness capability; most issues are rapidly detected from 24x7x365 monitoring and alarming of real time metrics and service dashboards. The majority of incidents are detected in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers.
    - Trouble ticket entered by an AWS employee.
    - Calls to the 24X7X365 technical support hotline – If the event meets incident criteria, then the relevant on-call support engineer will start an engagement utilizing AWS Event Management Tool system to start the engagement and page relevant program resolvers (e.g., Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause.
- Recovery Phase – The relevant resolvers will perform break fix to address the incident. Once troubleshooting, break fix, and affected components are addressed, the call leader will assign next steps in terms of follow -up documentation and follow-up actions and end the call engagement.
- Reconstitution Phase – Once the relevant fix activities are complete the call leader will declare that the recovery phase is complete. Post mortem and deep-root-cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and relevant actions, such as design changes etc., will be captured in a Correction of Errors (COE) document and tracked to completion.

In addition to the internal communication mechanisms detailed above, AWS has also implemented various methods of external communication to support its customer base and community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" (http://status.aws.amazon.com/) is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.

The AWS incident management program is reviewed by independent external auditors during audits for our System and Organization Controls (SOC), PCI DSS, ISO 27001 and Federal Risk and Authorization Management Program (FedRAMP) compliance. Additionally, the AWS incident response playbooks are maintained and updated to reflect emerging risks and lessons learned from past incidents. Plans are tested and updated through the due course of business (at least monthly).

3.1.3 SERVICENOW

ServiceNow strives to deliver safe and secure cloud services that you can rely on to run your business. Our state-of-the-art security infrastructure, data encryption techniques, and threat response processes ensure that your data is always protected and secure. Our advanced, high-

availability infrastructure and a multi-instance architecture provides you with cloud services that are reliable, configurable, and scalable. And we remain committed to adhering to one of the broadest portfolios of industry standards, and complying with privacy and safety mandates as they continue to evolve.

As a ServiceNow customer, you have control over the security of your instance and your data within the ServiceNow cloud services. You can choose from several data-at-rest encryption options, manage application-level role based access controls, and authentication mechanisms. As a customer, you are also contractually permitted to conduct an application-level penetration test against your sub-production instance every year.

In addition to supporting and maintaining active policy and compliance certification (such as, SSAE 16 SOC 1 Type 2 and SOC 2 Type 2, and FedRAMP Moderate JAB ATO), ServiceNow understands the importance of incident resolutions with our ServiceNow IT Service Management Services, which at the foundation supports workflows to include multiple methods of managing incidents from minor to mission critical with target initial response times applied.

Priority	Definition	Target Initial Response	Coverage
P1	Instance Unavailable	30 minutes	Continuous
P2	Mission-critical defect	2 hours	Continuous
P3	Significant request or defect	1 business day	Business hours
P4	Important request or defect	N/A	Varies

Table 6: ServiceNow Response Times

In the event of a confirmed Data Breach of customer data supplied to ServiceNow, ServiceNow will immediately notify the Red River Contract Manager, Phillip Wieser and he will then notify the customer (please see Section 4.1 Excellent Customer Service (8.4.1) on page 27).

ServiceNow shall take reasonable measures to promptly mitigate the cause of the Breach and shall take reasonable corrective measures to prevent future Breaches. As information is collected or otherwise becomes available to ServiceNow and unless prohibited by law, ServiceNow shall provide information regarding the nature and consequences of the Breach that are reasonably requested to allow Customer to notify affected individuals, government agencies and/or credit bureaus. Customer is solely responsible for determining whether to notify impacted Data Subjects and for providing such notice, and for determining if regulatory bodies or enforcement commissions applicable to Customer or Customer Data need to be notified of a Breach. These procedures are outline in our DPA and DSG which has been updated to meet the GDPR mandates.

3.2 Adware, Software or Marketing (8.3.2)

Utah Solicitation Number SK18008 Requirement: Pages 25-26
8.3.2 Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

Red River certifies we, and our partners at AppDynamics, AWS and ServiceNow, will not engage in, nor permit agents to, push adware, software, or marketing not explicitly authorized by the Participating Entity or the MSA.

3.3 User Test/Staging Environment (8.3.3)

Utah Solicitation Number SK18008 Requirement: Page 26
8.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production

Red River works with its clients on a case by case basis to provide the appropriate level of testing/staging environment based on needs and requirements.

3.3.1 AppDynamics

For the Software as a Service offering, the environments are identical for any environment in which the customer wishes to monitor.

3.3.2 AWS

With AWS, production systems may be easily cloned for use as development and test environments. Staging environments may be easily promoted to production.

3.3.3 ServiceNow

All ServiceNow customers are provided one production and one non-production instance. Customer may use the non-production instance as user test/staging or purchase additional non-production instances.

3.4 Access for People with Disabilities (8.3.4)

Utah Solicitation Number SK18008 Requirement: Page 26
8.3.4 Offeror must describe whether or not its computer applications and Web sites are accessible to people with disabilities, and must comply with Participating Entity accessibility policies and the Americans with Disability Act, as applicable.

Red River has more than 40 successful client engagements where applications and supporting infrastructure require compliance with accessibility requirements covered by Section 508 of the

Rehabilitation Act and Section 255 of the Communications Act. We are experienced in understanding Web Content Accessibility Guidelines (WCAG) 2.0 provisions and supporting clients in alignment with Levels of Success Criteria and Conformance Requirements.

Red River will comply with accessibility policies promulgated by any Participating Entities.

3.4.1 APPDYNAMICS

The UI is a web-based and adheres to accessibility standards and/or policies. Access to the AppDynamics UI is documented in a Section 508 Product Accessibility Template (VPAT - available upon request).

3.4.2 AWS

The AWS ElasticWolf Client Console has incorporated Section 508 requirements and AWS has prepared a Voluntary Product Accessibility Template (VPAT) for the Console, which outlines the Console's accessibility features. AWS offers the VPAT upon request.

AWS provides API-based cloud computing services with multiple interfaces to those services, including SDKs, IDE Toolkits, and Command Line Tools for developing and managing AWS resources. In addition, AWS provides two graphical UIs, the AWS Management Console and the AWS ElasticWolf Client Console.

3.4.3 SERVICENOW

ServiceNow alignment with Section 508 Web Content Accessibility Guidelines (WCAG) 2.0 Level A is outlined in the ServiceNow Kingston Release documentation (dated July 2018). The assistive technologies JAWS, NVDA, and VoiceOver are used to test ServiceNow products.

3.5 Applications and Web Browsers (8.3.5)

Utah Solicitation Number SK18008 Requirement: Page 26
8.3.5 Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at a minimum.

Red River has provided CSP-specific responses below.

3.5.1 APPDYNAMICS

The AppDynamics Controller UI is an HTML 5-based browser application that works best with the latest version of any modern browser. The Controller UI has been tested with and supports the last two versions of the following browsers:

- Safari

- Chrome
- Firefox
- Microsoft Edge
- Internet Explorer

A small number of screens in the Controller UI leverage Flash, and require Flash Player 10 or greater; AppDynamics recommends version 11. Certain types of ad blockers can interfere with features in the Controller UI. We recommend disabling ad blockers while using the Controller UI. IE users are advised to use IE 10+ versions when using the Controller UI. We also support a mobile application for iPhone, iPad, or other iOS-based devices version iOS 8.0 or higher and Android version 4.0 (Ice Cream Sandwich) or higher.

3.5.2 AWS

The following browsers are supported for the AWS Management Console:

Browser	Versions
Google Chrome	Latest three (3) versions
Mozilla Firefox	Latest three (3) versions
Microsoft Edge	Latest three (3) versions
Apple Safari for MacOS	Latest two (2) versions
Microsoft Internet Explorer	11

Table 7: AWS Browser Support

3.5.3 SERVICENOW

Most major browsers are supported by ServiceNow:

Browser	Versions
Google Chrome	Latest public release
Mozilla Firefox	Latest public release
Microsoft Edge	Latest public release
Apple Safari for MacOS	Latest public release
Microsoft Internet Explorer	11 and up

Table 8: ServiceNow Browser Support

3.6 Service Level Agreements (8.3.6)

Utah Solicitation Number SK18008 Requirement: Page 26
8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations

Red River will, prior to the execution of a Service Level Agreement (SLA), conduct the onboarding meetings with the Purchasing Entity and designees necessary to establish clarity on requirements and a detailed alignment between requirements and the appropriate SLA infrastructure. Our experience is that combining discussions around SLAs with initial discussions about the project management infrastructure is effective at confirming how and when SLA compliance is tracked from project start to initiation of operations and through the health of ongoing operations.

The objectives of our kickoff meetings include:

- Introducing team members, and points of contact with key stakeholders
- Establishing expectations and refining scope of effort
- Defining roles and responsibilities for each effort
- Highlighting critical timelines, tasks, milestones, or events
- Aligning reporting structures for SLAs and management status

During these meetings, Red River will work closely with the Participating Entity to determine whether any sensitive or personal information will be stored or used by Red River that is subject to any law, rule or regulation providing for specific compliance obligations.

3.6.1 AppDynamics

Red River has included the most current copy – as of June 29, 2018 – of the AppDynamics SLA in Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018) beginning on page 141. Due to the rapid evolution of cloud services, the latest AppDynamics SLAs are located at https://info.appdynamics.com/rs/031-WIX-618/images/AppDynamics%20SaaS%20Downloads%20EULA%2005-2018.pdf

AppDynamics will meet, upon request, of the customer to understand what data will be stored where. AppDynamics will also adhere to any laws, rules, or regulations to meet compliance and customer need.

3.6.2 AWS

Red River has included the most current copy - as of June 29, 2018 - of SLAs in appendices. Due to the rapid evolution of cloud services, links have been provided for potential updates after June 29, 2018:

- Amazon CloudFront SLA in Section 22 APPENDIX: Amazon CloudFront SLA (as of 6-29-2018) beginning on page 158 and http://aws.amazon.com/cloudfront/sla/
- Amazon EC2 (Compute) in Section 23 APPENDIX: Amazon EC2 SLA (as of 6-29-2018) beginning on page 162 and http://aws.amazon.com/ec2-sla/
- Amazon Dynamo DB in Section 24 APPENDIX: Amazon Dynamo DB SLA (as of 6-29-2018) beginning on page 167 and https://aws.amazon.com/dynamodb/sla/
- Amazon Relational Database Service (Amazon RDS) SLA in Section 25APPENDIX: Amazon RDS SLA (as of 6-29-2018) beginning on page 172 and http://aws.amazon.com/rds-sla/
- Amazon Route 53 SLA in Section 26 APPENDIX: Amazon Route 53 SLA (as of 6-29-2018) beginning on page 177 and http://aws.amazon.com/route53/sla/
- Amazon Simple Storage Service (Amazon S3) SLA in Section 27 APPENDIX: Amazon S3 SLA (as of 6-29-2018) beginning on page 182 and http://aws.amazon.com/s3-sla
- AWS Shield Advanced SLA Section 28APPENDIX: AWS Shield Advanced SLA (as of 6-29-2018) beginning on page 186 and https://aws.amazon.com/shield/sla/
- Traditionally, organizations establish SLAs and Operational Level Agreements (OLAs) through a series of negotiations between end users or portfolio owners and the operations team. Many organizations revisit expectations for their SLAs and OLAs due to the degree of change in capability. When following best practices for cloud adoption, customers often find that SLAs and OLAs for traditional things like uptime or availability for individual components will become irrelevant over time. Therefore, instead of reusing existing SLAs and OLAs for their cloud workloads, we encourage our customers to shift from an IT-centric view to a user-centric view of IT service delivery. Following best practice guidance, implementing automation, and reusing effective cloud architecture patterns gives development teams the ability to readily implement highly available solutions. With AWS's automated failure detection and recovery, systems can fail and recover without affecting users of the IT environment. AWS customers can build highly resilient systems in the cloud by employing multiple instances in multiple Availability Zones and data replication to achieve extremely high Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), and service availability.

3.6.3 SERVICENOW

Red River has included the most current copy - as of June 29, 2018 - of SLAs for the ServiceNow platform in Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018) beginning on page 217. Due to the rapid evolution of cloud services, links have been provided for potential updates after June 29, 2018:

- ServiceNow General Terms and Conditions
- ServiceNow Subscription Service indirectly from a reseller (e.g., via this NASPO/ValuePoint MSA) - Subscription Service Agreement
- ServiceNow Subscription Service Data Processing Addendum

3.7 Project Schedules/Work Plans (8.3.7)

Utah Solicitation Number SK18008 Requirement: Page 26
8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

Red River has developed and continually refines our InfoVision™ engagement management methodology – a repeatable, transparent, agile, structured, and consistent approach to successful delivery engagements. InfoVision™ was built to, and continues to evolve with, accepted industry standards, including the Project Management Book of Knowledge (PMBOK) and Scrum Alliance. At the same time, we value our ability to work with different clients that maintain their own methodology frameworks and/or may be at different levels of maturity in internal processes. For example, we have significantly tailored our InfoVision™ framework with State of California Agencies and Departments to verify our project processes are also compliant with California's Statewide Administrative Manual (SAM) and the California Department of Technology's Project Management Framework (CA-PMF).

Our approach involves direct interaction with the Participating Entity to determine "client-specific" protocols that must be held (e.g., required status formats for oversight agencies), level of documentation, frequency of interactions and other attributes that allow us to right-size the management infrastructure to the size, scale and complexity of the engagement. For example, our delivery engagement with the US Navy for AWS Migration requires a degree of management infrastructure more aligned with the PMBOK Program Management Professional (PgMP) scale whereas our engagement with the CA Health Benefit Exchange/Covered California (Covered CA) does not necessitate, per California's framework, the same degree of process and documentation – and both are highly successful engagements.

3.7.1 Project/Program Management Library

Red River has a library of project management samples and templates to draw from at contract execution that quickly allows Red River to "hit the ground running" on projects and related activities. A list of some of the typical plans and work products can include:

- Project Charter
- Project Management Plan
- Contract Management Plan
- Kickoff Presentations

- Schedule Management Plan
    - Project Schedule with Work Breakdown Structure (WBS) and critical path analysis
- Communication Management Plan
- Resource Management Plan
    - Project Organization
    - Staff Roles and Responsibilities
    - Onboarding Documents
- Risk and Issue Management Plans
    - Risk Registry Log
    - Issue Registry Log
    - Risk and Issue Intake Form
- Change Control Plan
    - Change Control Form
- Stakeholder Management Plan
    - Stakeholder Engagement Matrix
- Project Status Meeting and Reports
    - Meeting Agenda and Minutes
    - Steering Committee Meeting Briefing Summary
    - Monthly and Weekly Project Status Reports
- Transition to Maintenance and Operations Plan
- Other Project Templates
    - Decision Logs
    - Knowledge Transfer Log
    - Lessons Learned Session Matrix

3.7.2 PROJECT SCHEDULE VIEW

For project scheduling, Red River brings forth years of expertise in developing, managing, and controlling project schedules. Project schedule experience includes developing, refining, and managing simple to complex project schedules, within a variety of federal, state, local and commercial agencies, departments, and entities, and interfacing with few to many stakeholders. Figure 1: Representative Project Schedule provides a view of the framework we may use to initiate a client-specific tailoring process.

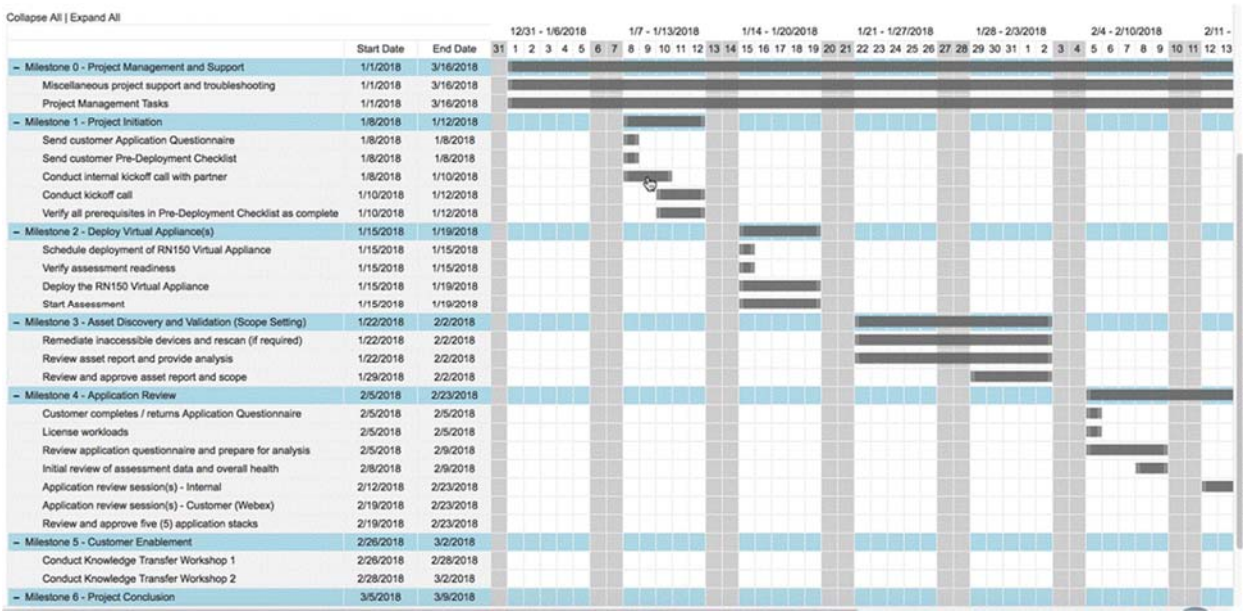


Figure 1: Representative Project Schedule

Red River uses industry-standard tools, such as Microsoft Project for schedule management or Jama software for requirements management and also has experience with a wide array of other tools and can adapt management processes around existing client toolsets.

3.7.3 EXECUTIVE ROADMAPS

InfoVision™ framework also incorporates executive level reporting tools that help translate the detailed schedule presentations necessary for project control with broader roadmaps more accessible for decision-makers. Figure 2: Representative Client Roadmap below provides an example of a higher-level roadmap we use for a more visual, executive representation of our Path to Cloud tasks and milestones.

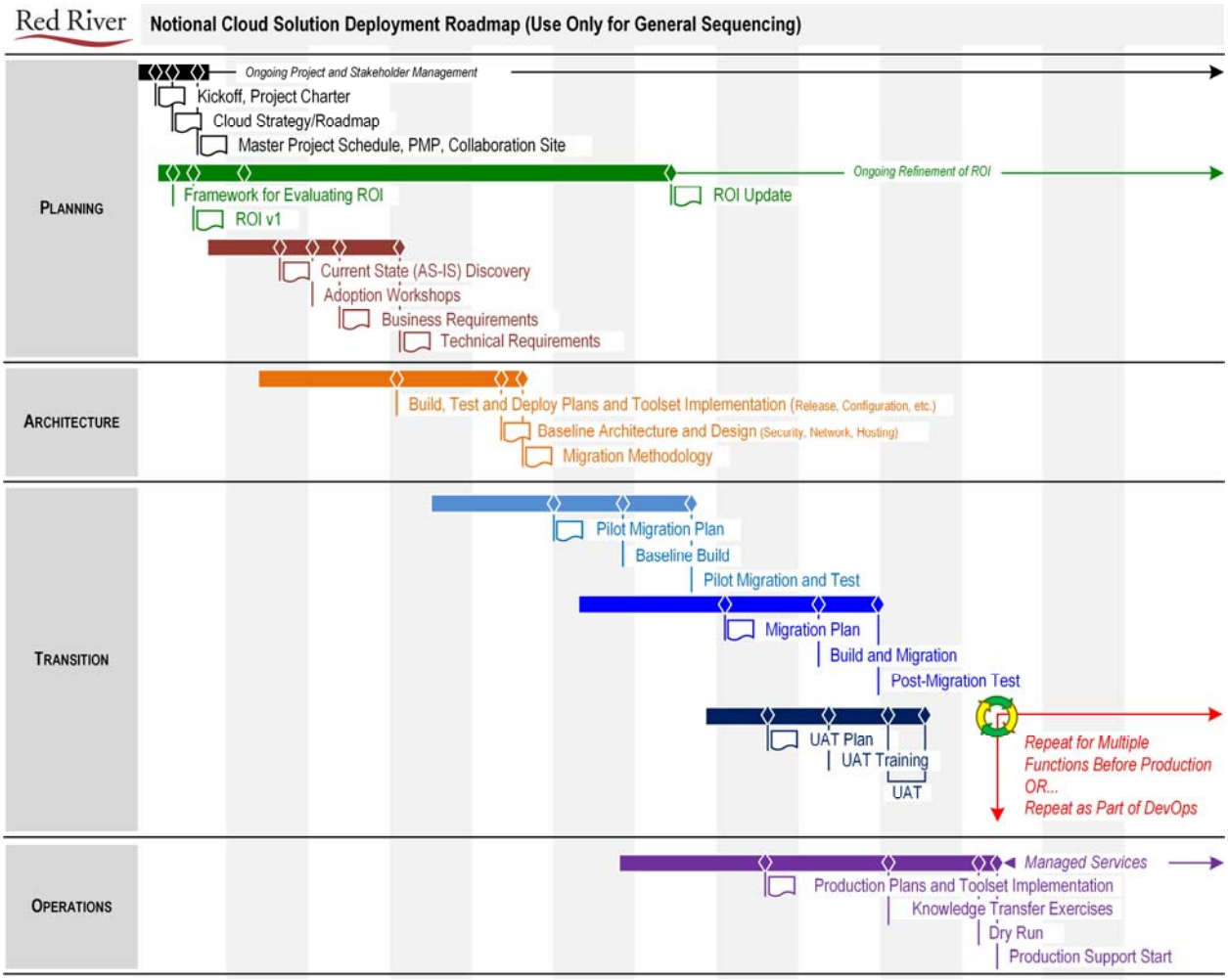


Figure 2: Representative Client Roadmap

In all our client engagements, we use these examples as a placemat for dialogue to "right-size" the project management infrastructure and approach. Red River understands there can be over-emphasis on project management processes that can inhibit a smaller-scale effort and pays close attention to the tools and processes appropriate to the scale and complexity of the effort.

3.8 Technology Changes (8.3.7)

Utah Solicitation Number SK18008 Requirement: Page 26
8.3.8 The State of Utah expects Offeror to update the services periodically as technology changes. Offer must describe:

- *How Offeror's services during Service Line Additions and Updates pursuant to section 2.12 will continue to meet the requirements outlined therein.*
- *How Offeror will maintain discounts at the levels set forth in the contract.*
- *How Offeror will report to the Purchasing Entities, as needed, regarding changes in technology and make recommendations for service updates.*
- *How Offeror will provide transition support to any Purchasing Entity whose operations may be negatively impacted by the service change.*

Red River's dedicated Engineering and Partner Management teams are continually interviewing new partners; staying abreast of new technology trends and Cloud methodologies; and tracking trends in SaaS Cloud offerings. Our Engineering organization attends routine technical training and briefings to stay informed on current and evolving technology. Sales teams are in the field daily talking with GSA customers and passing along new customer requirements for applicable addition to contract. Figure 3: Red River Technology Refresh Approach below highlights steps of our approach a high level.

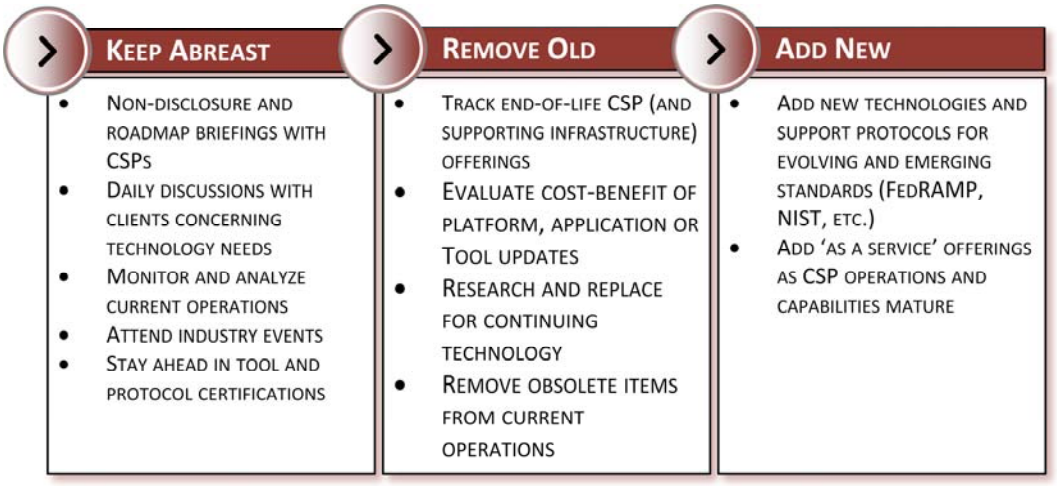


Figure 3: Red River Technology Refresh Approach

Red River utilizes the strategies outlined in Table 9: Red River Technology Change Strategies below to stay current on industry trends, including Cloud offerings. As we become aware of technology, we refresh our contracts accordingly. Red River's Innovation Center and Cloud Lab allows customers to try new technology.

Activity/Team	Description
Red River's Alliance Partner Management (APM) Team	Red River's Alliance Partner Management (APM) team is continually interviewing new partners and CSPs to add to our portfolio of supported technologies and make them available on contract.
Red River Innovation Center and Cloud Lab	• Sandbox for Customers to try before they buy • Center for innovation • Allows customers to try • Provide training on new technology to Red River engineers
Industry Participation	• VirtuStream/EMC VAR Council • Dell Partner Advisory Council
Red River Engineering Team	Red River's Engineering Organization attends routine training and briefings to stay informed on current and evolving technology. As they learn of upcoming technology releases from existing and new CSP partners, they work with the dedicated Red River Contract Managers to get the new technology added to the contract.

Table 9: Red River Technology Change Strategies

Under all circumstances, Red River will coordinate closely with the State of Utah, NASPO/ValuePoint and Participating Entities to identify technology changes, potential impacts to existing offerings and appropriate protocols for updates.

3.8.1 AppDynamics

During the term of the Master Agreement(s), AppDynamics may update or remove the awarded Solutions as service (with significant lead-time and communication with NASPO/ValuePoint and Participating Entities). Any new services that are introduced will meet the minimum specifications and terms and conditions outlined in the resulting master agreement and in AppDynamics' response. New additions with accompanying terms and conditions may not diminish or weaken existing terms and conditions in the judgment of the State of Utah (lead state).

- AppDynamics has the ability to offer "price lock" for customers that procure software via the UT NASPO agreement. AppDynamics offers standard 12, 24 and 36-month subscription service durations and can extend beyond these duration terms as approved by AppDynamics.
- AppDynamics will make resources available for half-yearly business and services updates and reviews to inform the Publishing Entities of any material changes to the offering. AppDynamics traditionally releases major version updates 2x annually, and AppDynamics plans to regularly and expediently update the Publishing Entities to any product changes.

- AppDynamics professional services and customer service teams have the ability to assist customers impacted by service changes. Subscription agreements entitle the user to have access to customer support during the time of active subscription. Due to the fact that the 'controller' will be hosted in the AppDynamics SaaS environment, our aim and goal is to make all feature changes non-disruptive to the end user. AppDynamics constantly strives to add features and functionalities via user requests and feature requests.

3.8.2 AWS

AWS's pace of innovation is funded and sustained through our economies of scale and commitment to delivering the products and services that matter most to our customers. Our continual innovation ensures that customers maintain "state of the art" IT infrastructure without having to make recapitalization investments. AWS development teams work directly with customers to ensure that innovation is driven by customer demand, and we continuously evolve and improve our existing services and frequently add new services. Customers can subscribe to receive information about the latest products, services, and feature announcements from AWS at: http://aws.amazon.com/new/.

3.8.3 SERVICENOW

ServiceNow works with its customers to ensure all technology updates and changes retain the high level of requirements originally agreed upon. As part of our ongoing development efforts to ensure latest security and industry trends are met and delivered in a timely fashion, we deliver and release families containing new features, enhancements and bug fixes approximately twice per year. ServiceNow maintains product support in the form of patches and hotfixes for the current family release and the past two releases (n-2). For older releases, product documentation and community support options are still available. Customer instances are patched on a quarterly schedule to ensure security, availability and performance. Patch targets are announced ahead of the quarter so the customer can plan.

4. (E) CUSTOMER SERVICE (8.4)

4.1 Excellent Customer Service (8.4.1)

Utah Solicitation Number SK18008 Requirement: Page 25
8.4.1 Offeror must describe how it will ensure excellent customer service is provided to Purchasing Entities. Include:

- *Quality assurance measures;*
- *Escalation plan for addressing problems and/or complaints; and*
- *Service Level Agreement (SLA)*

As outlined in Section 3.6 Service Level Agreements (8.3.6) and Section 3.7 Project Schedules/Work Plans (8.3.7), Red River values early interactions to outline our approach, learn the client's current structures and look-forward expectations and then collaboratively agree on processes we will employ for collective success.

Red River customers experience not only on-time every-time delivery and services, but also a friendly, collaborative culture that made us the successful contractor we are today. Our NASPO support team is in place and ready to begin performance immediately upon award - we have already established a direct communication band for NASPO/ValuePoint

- Single Point of Contact for Contract and Compliance – Phillip Weiser (see Red River Organization and Staffing document)
- Dedicated Phone Response through our 24x7x365 Managed Services organization – TBD
- Fully-supported NASPO email – NASPOCloudSolutions@RedRiver.com

As most of our customers will attest, and our past performance demonstrates, the innate culture of Red River is all about positive and productive relationships with our customers, partners, suppliers, and industry. From the first bullet of our Corporate Objectives, "Customer Service First" to our impeccable industry reputation for strong relationships with counterpart Federal program offices and contracting offices, such as:

- National Aeronautics and Space Administration (NASA) Solutions for Enterprise-Wide Procurement (SEWP) V NNG15SC85B (Group C-Small Business), NNG15SC46B (Group D)
- National Institutes of Health (NIH) National Institutes of Health Information Technology Acquisition and Assessment Center (NITAAC)
- US General Services Administration (GSA) FSS
- US Navy SPAWAR
- DHS Strategic Sourcing Program Office

Red River prides ourselves on our positive, can- do attitude in forging and maintaining strong relationships.

Red River can provide NASPO/ValuePoint and Purchasing Entities with a Red River "storefront" – an online portal for selecting, purchasing, provisioning, and de-provisioning services; migrating to and from the cloud; and engaging customer support. We provide Purchasing Entities with the ability to create a case themselves through the customer service portal or they can call our 24x7x365 managed services team to report their problem and have a case created.

As Red River engages with Participating Entities, we will clearly establish the expected communication and support protocols, such as online self-help, online support, telephone- based Help Desk services, real-time case management, or contracted custom support services. Our commitment to customer service is foremost, however, should we fail to meet agreed upon incident response times or the problem is not satisfactorily resolved, the user can escalate the problem, first by contacting their state liaison or directly engaging our Contract Manager.

4.1.1 APPDYNAMICS

AppDynamics will provide access to a ticketing system that will be available twenty-four (24) hours per day, seven (7) days per week. The ticketing system will be maintained by qualified support specialists, who shall use commercially reasonable efforts to provide technical support regarding the Software.

Error Resolution: If AppDynamics determines there is an error in the Software, AppDynamics may, at its sole option, repair that error in the version of the Software that End User is currently using or instruct End User to install a newer version of the Software with that error repaired. AppDynamics reserves the right to provide End User with a workaround in lieu of fixing an error.

☑ *Please refer to Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018) beginning on 141 for additional information on customer service expectations*

4.1.2 AWS

AWS Support is a one-on-one, fast-response support channel that is staffed 24x7x365 with experienced technical support engineers. The service helps customers of all sizes and technical abilities to successfully use the products and features provided by AWS. AWS Support provides a highly personalized level of service for customers seeking technical help. Customers who do not choose AWS Support will continue to have access to Basic Support offered at no additional charge. All plans, including Basic Support, provide 24x7 access to customer service, AWS Documentation, Resource Center, Product FAQs, Discussion Forums, and support for Health Checks. All customers receive Basic Support included with an AWS account.

For access to technical support and additional AWS Support resources, we offer plans to fit a customer's unique needs. A comparison between Basic, Developer, Business, and Enterprise

support is available in Table 10: AWS Customer Support Highlights, as well as on our Compare AWS Support Plans page.

4.1.2.1 AWS Support Pricing

All AWS Support tiers include an unlimited number of support cases, with no long-term contracts. Also, with the Business and Enterprise-level tiers, as your AWS charges grow, you earn volume discounts on your AWS Support costs. Please note that these calculations are performed on a per-account basis. Check out the Simple Monthly Calculator for a customized estimate of your deployment's AWS Support cost. For additional information on AWS Support pricing, visit the AWS Support Plan Pricing webpage.

4.1.2.2 Contacting AWS Support

Customers can contact AWS Support via the Support Center. All Developer-level support customers can open a case online with "Web Support" using a web browser. Business- and Enterprise-level customers may also "Click to Call" to have AWS contact them at any convenient phone number or strike up a conversation with an engineer via Chat. Enterprise-level customers also have a direct access to their dedicated TAM.

Chat is another way to contact AWS Support. By clicking on the chat support icon in the Support Center, a chat session will be initiated through the browser. This provides a real-time, one-on-one interaction with our support engineers and allows additional information and links to be shared for faster issue resolution.

Feature	Basic	Developer	Business	Enterprise
Customer Service – 24x7x365	✓	✓	✓	✓
Support Forums	✓	✓	✓	✓
Documentation, Whitepapers, Best Practice Guides	✓	✓	✓	✓
Access to Technical Support	• Support for Health Checks	• Email (local business hours)	• Phone • Chat • Email (24/7)	• Phone • Chat • Email • Technical Account Manager (TAM) (24/7)
Primary Case Handling	• Technical Customer Service Associate	• Cloud Support Associate	• Cloud Support Engineer	• Sr. Cloud Support Engineer

Feature	Basic	Developer	Business	Enterprise
Users Who Can Create Technical Support Cases	n/a	1	• Unlimited (AWS Identity and Access Management [IAM] supported)	• Unlimited (IAM supported)
Response Time	n/a	• General guidance: < 24 business hours • System impaired: < 12 business hours	• General guidance: < 24 hours • System impaired: < 12 hours • Production system impaired: < 4 hours • Production system down: < 1 hour	• General guidance: < 24 hours • System impaired: < 12 hours • Production system impaired: < 4 hours • Production system down: < 1 hour • Business-critical system down: < 15 minutes
Architecture Support	n/a	• General Guidance	• Contextual Use Case Guidance	• Contextual Application Architecture Guidance
Access to Support API	n/a	n/a	✓	✓
Third-Party Software Support	n/a	n/a	✓	✓
AWS Trusted Advisor	• 4 core checks	• 4 core checks	• Full checks	• Full checks
Infrastructure Event Management	n/a	n/a	• Contact Us for Pricing	✓
Direct Access to TAM	n/a	n/a	n/a	✓
Architectural Review	n/a	n/a	n/a	✓
Support Concierge	n/a	n/a	n/a	✓
Training	n/a	n/a	n/a	• Access to online self-paced labs
Operations Support	n/a	n/a	n/a	• Operational reviews, recommendations, and reporting

Table 10: AWS Customer Support Highlights

☑ *Please refer to AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

4.1.3 SERVICENOW

ServiceNow provides Customer Support 24 hours a day, 7 days week, 365 days a year. Support Centers are located in the US, UK, Netherlands, Australia and India, with applicable contact numbers or customers can directly enter a contact initiation form. ServiceNow provides customers with multiple methods of gaining support, quickly and efficiently:

- Knowledge Area to glean the latest alerts, best practices, and troubleshooting tips
- Documentation to visit site for latest product information and release notes
- Community forums to glean handy tips and product details from specific community members
- HI Service Portal to manage tasks, accounts, and incidents which are prioritized and responded to within the response time frames
- Known Error Portal to filter the known errors released via release notes

The ServiceNow Incident system is maintained by qualified support specialists, who provide technical support and triage for error resolution as per our partner agreements and SLAs.

☑ *Please see Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018) beginning on page 217 for more information on SLAs*

4.2 Complying with Customer Service Requirements (8.4.2)

Utah Solicitation Number SK18008 Requirement: Page 26	
8.4.2	*Offeror must describe its ability to comply with the following customer service requirements:* *a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.* *b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.* *c. Customer Service Representative will respond to inquiries within one business day.* *d. You must provide design services for the applicable categories.* *e. You must provide Installation Services for the applicable categories.*

Red River understands and will comply with customer service requirements under the broader NASPO/ValuePoint MSA and with each Participating Entity. Our Single Point-of-Contact for NASPO/ValuePoint contract and compliance issues is Phillip Weiser (see Red River Organization and Staffing document).

Mr. Weiser will tap the appropriate resources within Red River to define and verify compliance with customer service requirements outlined in any State Participating Addendum and associate client engagements. As the nature of engagements may vary, the nature of customer service channels may also vary – but under all circumstances – Red River will clearly identify the structures and personnel for a Single Point of Contact, customer service representatives available from 7AM to 6PM on Monday through Sunday for the client's time zones. We will leverage our 24x7x365 NOC as a standard entry point for requests and will adhere to requirements, such as responding to inquiries within at least one business day – and further tailor support to meet client expectations and requirements.

Red River has a long history of providing the continuum of cloud capabilities and services in our Path to Cloud – Planning, Architecture and Design, Transition and Ongoing Health Maintenance and will tailor the support model to meet client requirements and expectations. Our Red River team is staffed with trained customer service representatives and will be responsible for responding to inquires within one business day and held accountable to being available during the requested, or subsequently revised, working hours by phone or email to support NASPO/ValuePoint customers.

4.2.1 APPDYNAMICS

AppDynamics will provide access to a ticketing system that will be available twenty-four (24) hours per day, seven (7) days per week as detailed in Table 11: AppDynamics Response Times. The ticketing system will be maintained by qualified support specialists, who shall use commercially reasonable efforts to provide technical support regarding the Software.

Error	Initial Response & Acknowledgement	Manager Escalation	VP Escalation	Email Status Updates for Open Cases
Urgent	1 Hour	1 Business Day	1 Week	Daily
High	6 Hours	1 Week	2 Weeks	Weekly
Normal	1 Business Day	Quarterly Review for All Open Issues	None	None
Low	2 Business Days	Semi-Annual Review for All Open Issues	None	None

Table 11: AppDynamics Response Times

☑ *Please refer to Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018) beginning on page 141 for additional information on customer service expectations*

4.2.2 AWS

☑ *Please see our response to Section 4.1 Excellent Customer Service (8.4.1) Subsection 4.1.2 AWS above.*

☑ *Please also refer to AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

4.2.3 SERVICENOW

As indicated in Section 4.1 Excellent Customer Service (8.4.1) Subsection 4.1.3, ServiceNow additionally complies with this requirement by providing Customer Support 24 hours a day, 7 days week, 365 days a year either by phone, contact form, or through the **HI Service Portal** incident reporting system maintained by qualified support specialists who target timely response times as indicated in Table 12: ServiceNow Response Times.

Priority	Definition	Target Initial Response	Coverage
P1	Instance Unavailable	30 minutes	Continuous
P2	Mission-critical defect	2 hours	Continuous
P3	Significant request or defect	1 business day	Business hours
P4	Important request or defect	N/A	Varies

Table 12: ServiceNow Response Times

☑ *Please also see Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018) beginning on page 217 for more information on customer service expectations*

5. (E) SECURITY OF INFORMATION (8.5)

5.1 Protecting Data (8.5.1)

Utah Solicitation Number SK18008 Requirement: Page 26
8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services

Red River, and each of our proposed CSPs, subscribe to the shared responsibility model:

- Customers continue to own their data
- Customers choose the geographic location(s) in which to store their data—it does not move unless the customer decides to move it.
- Customers can download or delete their data whenever they like.
- Customers should consider the sensitivity of their data, and decide if and how to encrypt the data while it is in transit and at rest.

Each CSP provides customers with the ability to delete their data. However, customers retain control and ownership of their data, and it is the customer's responsibility to manage their data. Similarly, it is the customer's responsibility to provision/deprovision resources.

5.1.1 APPDYNAMICS

AppDynamics values trust and is committed at all levels to the security and privacy of data. AppDynamics has established a Security and Privacy Standard that describes the purpose for which PII is collected, used, retained, maintained, and shared.

☑ *Please see Section 31 APPENDIX: AppDynamics Security and Privacy Standard - CONFIDENTIAL beginning on page 243 for the current (as of 6/29/2018) standards documentation*

☑ *Please also see https://www.appdynamics.com/privacy-policy/ for continuing updates*

5.1.2 AWS

Because AWS customers retain ownership and control over their content within the AWS environment, they also retain responsibilities relating to the security of that content as part of the AWS "shared responsibility" model. While AWS manages security of the cloud, security in the cloud is the responsibility of the customer, as customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks – no differently than they would for applications in an on-site data center.

To assist customers in designing, implementing and operating their own secure AWS environment, AWS provides a wide selection of security tools and features customers can use.

Customers can also use their own security tools and controls, including a wide variety of third party security solutions. Customers can configure their AWS services to leverage a range of such security features, tools and controls to protect their content, including sophisticated identity and access management tools, security capabilities, encryption and network security.

AWS does not access or use customer content for any purpose other than as legally required and to provide the AWS services selected by each customer, to that customer and its end users. AWS never uses customer content or derives information from it for other purposes such as marketing or advertising.

5.1.3 SERVICENOW

ServiceNow's commitment to the protection of data is demonstrated in our certifications both internationally and within the United States, SSAE 16 SOC 1 Type 2 and SOC 2 Type 2 which is independently audited on an annual basis. We are committed to customer data protection and to that end has made significant investments in technology, processes, and expertise to ensure that our cloud services meet the most stringent of standards for security, availability, scalability, privacy, and compliance. As indicated, data security is paramount to us, ServiceNow employs various encryption techniques in our product families, such as:

- Encryption in Flight: As a customer, browser-based sessions to your ServiceNow cloud instance(s) are encrypted over the internet via Transport Layer Security (TLS) using AES-128 or AES-256 block ciphers.
- Integration Encryption: We can apply encryption to integrations, such as LDAP and Web Services, as well as commonly used file transfer methods.
- Email Encryption: We support opportunistic Transport Layer Security for email sent or received by a ServiceNow instance.
- Column-Level Encryption: We support AES-128, AES-256, and 3DES encryption algorithms, and apply your choice to encrypt data.
- Edge Encryption: Unencrypted target data is never stored in your ServiceNow instance. It provides you with the capability for automatic key rotation. It supports tokenization and substitution of data, such as credit card or social security numbers, to match standard data structures.
- Full Disk Encryption: Allows for everything inside the co-location spaces are owned, operated, and managed by ServiceNow. This includes the management of hard drives and server hardware. All hard drives are sanitized prior to leaving our private cages (per NIST 800-88 guidelines) which ensures your data is appropriately handled and protected. You can choose to further mitigate data exposure caused by the loss or theft of storage devices with AES-256 full-disk encryption of your data at rest.

ServiceNow believes in the shared responsibility model and the ServiceNow customer has control over the security of their instance and data within the ServiceNow cloud services. A single data classification is applied to all customer data we host. We do not inspect or monitor the data. The client applies access controls to restrict access in accordance with client-specific data classification policies.

ServiceNow clients decide what information is to be stored, how it is to be used, and how long it is retained. All data is hosted on solid-state or mechanical disks within our co-location spaces - No tapes or other forms of removable media are used to provide the service, including for backups.

When functional storage devices reach their end-of life or get reassigned to new customers, they are shredded based on guidance from NIST. Throughout the lifetime of your subscription, your data can be directly exported from the ServiceNow instance. This can be via the UI, through integrations, or by using other ServiceNow components. We return all your data in an SQL dump format at the end of a contract. All backed-up data is automatically deleted and overwritten 45 days from the end of a contract.

☑ *Please also see Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018) beginning on page 217 for data-related addenda*

5.2 Complying with Applicable Laws (8.5.2)

Utah Solicitation Number SK18008 Requirement: Page 27
8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security

Red River's broad experience with far more than 50 engagements with moderate or high data security provisions and across public-sector agencies with unique domain-specific data privacy and security requirements. Our corporate operations are ISO 9001:2015 and System and Organization Controls (SOC) 2 Type 1 certified and we have had direct, "hands-on" expertise with identifying, documenting and maintaining clear adherence to:

- FedRAMP, highlighted by our work with the US Navy, US GSA, CHSRA, CA SOS and Covered CA
- NIST, highlighted by our work with the STRATCOM, US Navy, US GSA, NV SSHIX, and Covered CA
- FISMA, highlighted by our work with the STRATCOM multiple major engagements with entities within the US DoD
- Health Insurance Portability and Accountability Act (HIPAA)
- Internal Revenue Service (IRS) Publication 1075
- Defense Information Systems Agency (DISA) highlighted by multiple major engagements with entities within the US DoD
- PCI DSS

Our more 40 projects in CA State Agencies and Departments have required compliance to some, or all, of the industry standards above, but also the State of California Statewide Administrative Manual (SAM) and Statewide Information Management Manual (SIMM). Our experience in 15

other state engagements is similar – there are unique policies and procedures with slight – or significant – variations unique to the state and/or domain.

Red River's project infrastructure specifically collects, documents and provides traceability to the appropriate laws, regulations and implementing polices using a requirements management tool. All our efforts are conducted in good faith to capture the relevant security standards and verify that our clients specifically confirm that we are collectively addressing the appropriate requirements.

5.2.1 AppDynamics

The AppDynamics Security Assurance, Legal, and Privacy teams are responsible for ensuring security, privacy, and legal compliance and providing guidance on information security, privacy, and regulatory risk and any appropriate mitigations. To support this work, these teams maintain relevant professional certifications and association memberships (i.e., CISSP, law licenses, engage outside counsel as we see needed, and IAPP), regularly engage outside counsel for additional advice, and work closely with our parent company, Cisco Systems, Inc., to supplement guidance, seek feedback, and share resources.

5.2.2 AWS

AWS Compliance enables customers to understand the robust controls in place at AWS that facilitate security and data protection in the cloud. The AWS Cloud infrastructure has been designed and is managed in alignment with regulations, standards, and best practices, including:

- Federal Risk and Authorization Management Program (FedRAMP)
- System and Organization Controls (SOC) 1, SOC 2, and SOC 3
- PCI DSS
- International Organization for Standardization (ISO) 27001, 27017, 27018, and 9001
- Department of Defense (DoD) Security Requirements Guide (SRG) Impact Levels 2, 4, 5, and 6
- Federal Information Security Management Act (FISMA)
- US Health Insurance Portability and Accountability Act (HIPAA)
- FBI Criminal Justice Information Services (CJIS)
- NIST 800-171
- International Traffic in Arms Regulations (ITAR)
- Federal Information Processing Standard (FIPS) 140-2
- Family Educational Rights and Privacy Act (FERPA)
- Information Security Registered Assessors Program (IRAP) (Australia)
- IT-Grundschutz (Germany)

For information on all of the security regulations and standards with which AWS complies, visit the AWS Compliance page.

5.2.3 SERVICENOW

ServiceNow adheres to industry best practices and regulatory requirements, including:

- FedRAMP Moderate JAB ATO
- SSAE SOC 1 Type 2 and SOC 2 Type
- PCI DSS
- ISO 27001
- ISO/IEC 27018
- Pink Verify (ITIL processes)
- Federal Information Security Management Act (FISMA)
- Multi-Tier Cloud Security (MTCS) for ISO 27001/02
- NIST 800-171
- General Data Protection Regulation (EU) and EU Privacy Shield
- Australian Signals Directorate (ASD) and registered under IRAP as a cloud service provider suitable for Australian government organizations

5.3 Access to a Purchasing Entity's Accounts (8.5.3)

Utah Solicitation Number SK18008 Requirement: Page 27
8.5.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement

Red River has expertise in the industry best practices of a shared data responsibilities model out lined in above – Customers own their data, choose location(s) to store their data, can download or delete their data, make the final decision on the sensitivity of their data, and decide if and how to their users will access their data.

Red River will use customer accounts and data only in the processing of an order and management of the customer's service entitlements – under no circumstances will Red River or the proposed CSPs use customer information outside of clearly-defined operating procedures.

5.3.1 APPDYNAMICS

AppDynamics Operations teams are not provided access into Purchasing Entity's user accounts or data. The Operations teams can see the management logs, however, if required may as the

Purchasing Entity to setup a temporary account to access the UI and data within a tenancy for troubleshooting purposes.

5.3.2 AWS

☑ *Please see our response to Section 5.1 Protecting Data (8.5.1) Subsection 5.1.2 AWS above*

5.3.3 SERVICENOW

ServiceNow sees compliance as a shared responsibility with clients - requirements such as greater data access and erasure rules, privacy by design, and data breach notification processes are important to understand.

☑ *Please see our response to Section 5.1 Protecting Data (8.5.1) Subsection 5.1.3 ServiceNow on page 35*

.

6. (E) PRIVACY AND SECURITY (8.6)

6.1 Compliance with Industry Standards (8.6.1)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.1 Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in Attachment D, including supporting the different types of data that you may receive

Red River has only proposed CSPs that comply with NIST SP 800-145 and other relevant industry standards – and is prepared to work collaboratively with clients and CSRs to verify the specific target list of additional standards that may be unique to the engagement.

☑ *Please refer to the following sections for elaboration of industry standards*
- *Section 1.1 NIST Special Publication 800-145 (8.1.1) beginning on page 2*
- *Section 1.2 Compliance with Attachment C NIST Service Models & Attachment D Scope of Services (8.1.2) beginning on page 5*
- *Section 1.3 Adherence to Attachment D Scope of Services (8.1.3) beginning on page 5*
- *Section 3.1 Data Breach (8.3.1) beginning on page 11*
- *Section 5 (E) SECURITY OF INFORMATION (8.5) beginning on page 34*

6.1.1 APPDYNAMICS

☑ *Please see our response to Section 1.1 NIST Special Publication 800-145 (8.1.1) Subsection 1.1.1 AppDynamics*

☑ *Please see our response to Section 5.2 Complying with Applicable Laws (8.5.2) Subsection 5.2.1 AppDynamics*

6.1.2 AWS

☑ *Please see our response to Section 1.1 NIST Special Publication 800-145 (8.1.1) Subsection 1.1.2 Amazon Web Services (AWS)*

☑ *Please see our response to Section 5.2 Complying with Applicable Laws (8.5.2) Subsection 5.2.2 AWS*

6.1.3 SERVICENOW

ServiceNow applies the same data classification for all hosted customer data. ServiceNow does not inspect or monitor its customers' information and therefore has no ability to sub-classify customer data. The overriding requirement of the assigned classification is that customer data remains hosted in the private cloud until the customer terminates their subscription. It is never stored anywhere apart from the private cloud. Customers remain the data owner and data

controller for all data placed into their instance. ServiceNow does not examine, inspect, monitor or analyze customers' data. Customers apply access controls to restrict access to data within their instances based on their own requirements and needs, including their own data classification.

☑ *Please see our response to Section 1.1 NIST Special Publication 800-145 (8.1.1) Subsection 1.1.3 ServiceNow*

☑ *Please see our response to Section 5.2 Complying with Applicable Laws (8.5.2) Subsection 5.2.3 ServiceNow*

6.2 Security Certifications (8.6.2)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

Red River's corporate operations are ISO 9001:2015 and System and Organization Controls (SOC) 2 Type 1 certified. We have direct planning, architecture and design, transition and ongoing health maintenance operations with the following standards:

- Content Delivery and Security Association (CDSA)
- Criminal Justice Information Services (CJIS)
- Defense Information Systems Agency (DISA)
- Family Educational Rights and Privacy Act (FERPA)
- Federal Information Processing Standard (FIPS) PUB 140-2
- FedRAMP
- FISMA
- Health Insurance Portability and Accountability Act (HIPAA)
- Internal Revenue Service (IRS) Publication 1075
- Multi-Level Protection Scheme (MLPS)
- NIST, notably 800-145 and the extending Cloud Reference Architecture in NIST 500-292
- PCI DSS
- US Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 Part 11

6.2.1 AppDynamics

AppDynamics undergoes a strict auditing process twice a year to ensure that all controls across AppDynamics' entire company demonstrate SOC 2 compliance and has been audited and approved by an independent auditing firm. Customers may request the AppDynamics' SOC 2 report at any time. AppDynamics agents by default do not capture, communicate nor store any personally identifiable information (PII/PHI) nor payment information, which may be related to a user request or business transaction. This includes data contained in HTTP request parameters and SQL bind variables.

AppDynamics can be configured to be fully compatible with most major compliance regulations including PCI-DSS, HIPAA, CA SB1386, and FISMA. AppDynamics' data center provider is also SOC 2 Type II compliant. In addition, AppDynamics is EU Safe Harbor certified and our hosted solution is managed by a third-party data center provider that is SAAS 70 and SAAS16 compliant. Also, AppDynamics is "In Process" (as of 06/27/2018) on the FedRAMP certification as documented on https://marketplace.fedramp.gov/#/product/appdynamics-by-cisco.

☑ *Please see our response to Section 5.2 Complying with Applicable Laws (8.5.2) Subsection 5.2.1 AppDynamics*

6.2.2 AWS

☑ *Please see our response to Section 1.1 NIST Special Publication 800-145 (8.1.1) Subsection 1.1.2 Amazon Web Services (AWS)*

☑ *Please see our response to Section 5.2 Complying with Applicable Laws (8.5.2) Subsection 5.2.2 AWS*

6.2.3 ServiceNow

☑ *Please see our response to Section 1.1 NIST Special Publication 800-145 (8.1.1) Subsection 1.1.3 ServiceNow*

☑ *Please see our response to Section 5.2 Complying with Applicable Laws (8.5.2) Subsection 5.2.3 ServiceNow*

6.3 Security Practices (8.6.3)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

In a traditional datacenter model, the client controls networked systems - the CSP model emphasizes a shared responsibility. Clients do not have physical access, but they do retain responsibility for networking and logical equivalent within their cloud environment. Red River and our proposed CSPs are well known for protecting trust and for investing in their security infrastructures. These include multiple levels of built-in security and multi-layer security architecture options customers can superimpose on top of their cloud environment.

6.3.1 AppDynamics

Access to the AppDynamics SaaS platform infrastructure and data is secured by multiple authentication challenges including RSA and DSA key pairs, passwords, and network access control lists. Infrastructure and data access is restricted to AppDynamics employees and contractors, all of whom are under strict confidentiality agreements. System and Network activity is actively monitored by a team of engineers 24/7. Failed authentication attempts are audited and engineers are paged immediately so that any possible intrusion or threat can be investigated promptly. Standard firewall policies are deployed to block all access except to ports required for AppDynamics SaaS platform and agent communication.

AppDynamics has provided with these responses a copy of its Security and Privacy Standard, a copy of its most recent SOC 2 report prepared by an independent auditor, as well its responses to the Cloud Security Alliance's CAIQ, all of which go into detail about the security controls in place.

6.3.2 AWS

AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used so personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

Documentation is maintained to aid and inform operations personnel in handling incidents or issues. If the resolution of an issue requires collaboration, a conferencing system is used which supports communication and logging capabilities. Trained call leaders facilitate communication and progress during the handling of operational issues that require collaboration. Post-mortems

are convened after any significant operational issue, regardless of external impact, and Cause of Error (COE) documents are drafted so the root cause is captured and preventative actions are taken in the future. Implementation of the preventative measures is tracked during weekly operations meetings.

AWS security monitoring tools help identify several types of denial of service (DoS) attacks, including distributed, flooding, and software/logic attacks. When DoS attacks are identified, the AWS incident response process is initiated. In addition to the DoS prevention tools, redundant telecommunication providers at each region as well as additional capacity protect against the possibility of DoS attacks.

The AWS network provides significant protection against traditional network security issues, and you can implement further protection. The following are a few examples:

- **Distributed Denial of Service (DDoS) Attacks.** AWS API endpoints are hosted on large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used. Additionally, AWS's networks are multi-homed across a number of providers to achieve Internet access diversity.
- **Man in the Middle (MITM) Attacks.** All of the AWS APIs are available via SSL-protected endpoints which provide server authentication. Amazon EC2 AMIs automatically generate new SSH host certificates on first boot and log them to the instance's console. You can then use the secure APIs to call the console and access the host certificates before logging into the instance for the first time. We encourage you to use SSL for all of your interactions with AWS.
- **IP Spoofing.** Amazon EC2 instances cannot send spoofed network traffic. The AWS-controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.
- **Port Scanning**. Unauthorized port scans by Amazon EC2 customers are a violation of the AWS Acceptable Use Policy. Violations of the AWS Acceptable Use Policy are taken seriously, and every reported violation is investigated. Customers can report suspected abuse via the contacts available on our website at: http://aws.amazon.com/contact-us/report-abuse/. When unauthorized port scanning is detected by AWS, it is stopped and blocked. Port scans of Amazon EC2 instances are generally ineffective because, by default, all inbound ports on Amazon EC2 instances are closed and are only opened by you. Your strict management of security groups can further mitigate the threat of port scans. If you configure the security group to allow traffic from any source to a specific port, then that specific port will be vulnerable to a port scan. In these cases, you must use appropriate security measures to protect listening services that may be essential to their application from being discovered by an unauthorized port scan. For example, a web server must clearly have port 80 (HTTP) open to the world, and the administrator of this server is responsible for the security of the HTTP server software, such as Apache. You may request permission to conduct vulnerability scans as required to meet your specific compliance requirements. These scans must be limited to your own instances and must not violate the AWS Acceptable Use Policy. Advanced approval for these types of scans

can be initiated by submitting a request via the website at: https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/AWSSecurityPenTestRequest

- **Packet sniffing by other tenants.** It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. While you can place your interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same customer located on the same physical host cannot listen to each other's traffic. Attacks such as ARP cache poisoning do not work within Amazon EC2 and Amazon VPC. While Amazon EC2 does provide ample protection against one customer inadvertently or maliciously attempting to view another's data, as a standard practice you should encrypt sensitive traffic.

6.3.3 SERVICENOW

The ServiceNow cloud is built for the enterprise customer with every aspect aimed towards meeting the customer's demand for reliability, availability and security. ServiceNow's comprehensive approach to address this demand is enabled by the following:

- ServiceNow's robust cloud infrastructure runs on its own applications and utilizes industry best-of-breed technology to automate mission critical functionalities in the cloud service with around-the-clock and around-the-world delivery;
- ServiceNow achieves flexibility and control in its ability to deliver a stable user experience to the customer by having a logical single tenant architecture;
- ServiceNow's application development which has a paramount focus on quality, security, and the user experience is closely connected to the operations of delivering those applications in a reliable and secure cloud environment;
- ServiceNow invests in a comprehensive compliance strategy that allows its customers to attain their own compliance to applicable laws by obtaining attestations and certifications and running its subscription service from paired data centers situated close to where its customers are located; and
- ServiceNow's homogeneous environment where all applications are on a single platform offers ServiceNow a competitive advantage in being able to concentrate its efforts to make the customer's user experience the best possible.

ServiceNow provides multiple methods of security adhering to NIST Standards, including such data in-flight encryption whereby as a ServiceNow customer, browser-based sessions to your ServiceNow cloud instance(s) are encrypted over the internet via Transport Layer Security (TLS) using AES-128 or AES-256 block ciphers and all end-user access to a ServiceNow instance is always automatically redirected to HTTPS if attempted over HTTP.

ServiceNow can apply encryption to integrations, such as LDAP and Web Services, as well as commonly used file transfer methods. In the case of an LDAPS over SSL connection, you can conveniently store certificates for specific LDAP servers within a ServiceNow instance for use in

signing instance-bound Web Service requests. We also support certificate-based mutual Web Services security authentication with external endpoints for all ServiceNow instances. Data can be securely transferred to your ServiceNow instances using pre-defined file transfer integration methods. You can also use clear text protocols such as FTP or HTTP to transfer data or support specific tasks, such as an approval or status request.

ServiceNow Encryption-at-rest security methods include Column level encryption, including support for AES-128, AES-256, and 3DES encryption algorithms, which can apply your choice to encrypt data. To mitigate the possible compromise of encrypted customer data, we re-encrypt (wrap) your keys with a secondary key.

With Edge Encryption, unencrypted target data is never stored in your ServiceNow instance. It provides you with the capability for automatic key rotation. It supports tokenization and substitution of data, such as credit card or social security numbers, to match standard data structures. Full Disk Encryption allows for everything inside the co-location spaces are owned, operated, and managed by ServiceNow. This includes the management of hard drives and server hardware. All hard drives are sanitized prior to leaving our private cages (per NIST 800-88 guidelines) which ensures your data is appropriately handled and protected. You can choose to further mitigate data exposure caused by the loss or theft of storage devices with AES-256 full-disk encryption of your data at rest.

6.4 Data Confidentiality Standards (8.6.4)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc)

Red River's SOC 1 Type 2 audit report attests to the design and health operations of our internal corporate infrastructure. Each of our proposed CSPS is audited annually to ensure compliance with the standards set by governments and the industry as noted in the Section above.

6.4.1 APPDYNAMICS

☑ *Please see our response to Section 5.1 Protecting Data (8.5.1) Subsection 5.1.1 AppDynamics*

6.4.2 AWS

AWS does not access customer data, and customers are given the choice as to how they store, manage and protect their data

☑ *Please see our response to Section 5.1 Protecting Data (8.5.1) Subsection 5.1.2 AWS*

6.4.3 SERVICENOW

ServiceNow does not inspect or monitor its customers' information and therefore has no ability to sub-classify customer data. The overriding requirement of the assigned classification is that customer data remains hosted in the private cloud until the customer terminates their subscription. It is never stored anywhere apart from the private cloud. Customers remain the data owner and data controller for all data placed into their instance. Customers apply access controls to restrict access to data within their instances based on their own requirements and needs, including their own data classification.

☑ *Please see our response in Section 5.1 Protecting Data (8.5.1) Subsection 5.1.3 ServiceNow*

6.5 Third-Party Certifications (8.6.5)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp High, FedRamp Moderate, etc.), and certifications relating to data security, integrity, and other controls.

Red River's corporate operations are ISO 9001:2015 and System and Organization Controls (SOC) 2 Type 1 certified. We have obtained FedRAMP ATOs for our clients and have facilitated client's obtaining confirmation of compliance with FISMA, HIPAA, IRS Pub 1075 and PCI-DSS.

6.5.1 APPDYNAMICS

AppDynamics undergoes a strict auditing process twice a year to ensure that all controls across AppDynamics' entire company demonstrate SOC 2 compliance and has been audited and approved by an independent auditing firm. Customers may request the AppDynamics' SOC 2 report at any time. AppDynamics agents by default do not capture, communicate nor store any personally identifiable information (PII/PHI) nor payment information, which may be related to a user request or business transaction. This includes data contained in HTTP request parameters and SQL bind variables.

AppDynamics can be configured to be fully compatible with most major compliance regulations including PCI-DSS, HIPAA, CA SB1386, and FISMA. AppDynamics' data center provider is also SOC 2 Type II compliant. In addition, AppDynamics is EU Safe Harbor certified and our hosted solution is managed by a third-party data center provider that is SAAS 70 and SAAS16 compliant. Also, AppDynamics is "In Process" on the FedRAMP certification as documented on https://marketplace.fedramp.gov/#/product/appdynamics-by-cisco.

☑ *Please see our response to Section 5.2 Complying with Applicable Laws (8.5.2) Subsection 5.2.1 AppDynamics and Section 6.2 Security Certifications (8.6.2) Subsection 6.2.1 AppDynamics*

6.5.2 AWS

☑ *Please see our response to Section 5.2 Complying with Applicable Laws (8.5.2) Subsection 5.2.2 AWS and Section 6.2 Security Certifications (8.6.2) Subsection 6.2.2 AWS*

6.5.3 SERVICENOW

☑ *Please see our response to Section 5.2 Complying with Applicable Laws (8.5.2) Subsection 5.2.3 ServiceNow and Section 6.2 Security Certifications (8.6.2) Subsection 6.2.3 ServiceNow*

6.6 Logging Process (8.6.6)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

6.6.1 APPDYNAMICS

AppDynamics' application server and machine software agents collect metrics that relate to the performance, health and resource of an application, its components (transactions, code libraries) and related infrastructure (nodes, and tiers) that service those components.

All data is securely transferred via HTTPS (TLS 1.2) from the agents back to the AppDynamics SaaS environment. The data is then processed and stored securely in encrypted format within the AppDynamics databases.

6.6.2 AWS

The logging and monitoring of Application Program Interface (API) calls are key components in security and operational best practices, as well as requirements for industry and regulatory compliance. AWS customers can leverage multiple AWS features and capabilities, along with third-party tools, to monitor their instances and manage/analyze log files.

6.6.2.1 AWS CloudTrail

AWS CloudTrail is a web service that records API calls to supported AWS services in an AWS account, delivering a log file to an Amazon Simple Storage Service (Amazon S3) bucket. AWS

CloudTrail alleviates common challenges experienced in an on-premise environment by making it easier for customers to enhance security and operational processes while demonstrating compliance with policies or regulatory standards.

With AWS CloudTrail, customers can get a history of AWS API calls for their account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.

- For information on the services and features supported by AWS CloudTrail, visit the AWS CloudTrail FAQs on the AWS website.
- The AWS whitepaper *Security at Scale: Logging In AWS* provides an overview of common compliance requirements related to logging, detailing how AWS CloudTrail features can help satisfy these requirements.
- The AWS whitepaper *Auditing Security Checklist for Use of AWS* provides customers with a checklist to assist in evaluating AWS for the purposes of an internal review or external audit.

6.6.2.2 AWS CloudTrail: Features and Benefits

Some of the many features of AWS CloudTrail include:

- Increased Visibility: AWS CloudTrail provides increased visibility into user activity by recording AWS API calls. Customers can answer questions such as, what actions did a given user take over a given time period? For a given resource, which user has taken actions on it over a given time period? What is the source IP address of a given activity? Which activities failed due to inadequate permissions?
- Durable and Inexpensive Log File Storage: AWS CloudTrail uses Amazon S3 for log file storage and delivery, so log files are stored durably and inexpensively. Customers can use Amazon S3 lifecycle configuration rules to further reduce storage costs. For example, customers can define rules to automatically delete old log files or archive them to Amazon Glacier for additional savings.
- Easy Administration: AWS CloudTrail is a fully managed service; customers simply turn on AWS CloudTrail for their account using the AWS Management Console, the Command Line Interface, or the AWS CloudTrail SDK and start receiving AWS CloudTrail log files in the specified Amazon S3 bucket.
- Notifications for Log File Delivery: AWS CloudTrail can be configured to publish a notification for each log file delivered, thus enabling customers to automatically take action upon log file delivery. AWS CloudTrail uses the Amazon Simple Notification Service (Amazon SNS) for notifications.
- Choice of Partner Solutions: Multiple partners including AlertLogic, Boundary, Loggly, Splunk, and Sumologic offer integrated solutions to analyze AWS CloudTrail log files.

These solutions include features like change tracking, troubleshooting, and security analysis. For more information, see the AWS CloudTrail partners section.

- Log File Aggregation: AWS CloudTrail can be configured to aggregate log files across multiple accounts and regions so that log files are delivered to a single bucket. For detailed instructions, refer to the Aggregating CloudTrail Log Files to a Single Amazon S3 Bucket section of the user guide.

6.6.2.3 Amazon CloudWatch

Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS DB instances, as well as custom metrics generated by customer applications and services, and any log files that applications generate. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react and keep their application running smoothly.

Customers can use CloudWatch Logs to monitor and troubleshoot systems and applications using their existing system, application, and custom log files. Customers can send their existing system, application, and custom log files to CloudWatch Logs and monitor these logs in near real-time. This helps customers better understand and operate their systems and applications, and they can store their logs using highly durable, low-cost storage for later access.

6.6.2.4 LogAnalyzer for Amazon CloudFront

LogAnalyzer allows customers to analyze their Amazon CloudFront Logs using Amazon Elastic MapReduce (Amazon EMR). Using Amazon EMR and the LogAnalyzer application customers can generate usage reports containing total traffic volume, object popularity, a breakdown of traffic by client IPs, and edge location. Reports are formatted as tab delimited text files, and delivered to the Amazon S3 bucket that customers specify.

Amazon CloudFront's Access Logs provide detailed information about requests made for content delivered through Amazon CloudFront, AWS's content delivery service. The LogAnalyzer for Amazon CloudFront analyzes the service's raw log files to produce a series of reports that answer business questions commonly asked by content owners.

6.6.2.5 Reports Generated

This LogAnalyzer application produces four sets of reports based on Amazon CloudFront access logs. The Overall Volume Report displays total amount of traffic delivered by CloudFront over the course of whatever period specified. The Object Popularity Report shows how many times each customer object is requested. The Client IP report shows the traffic from each different Client IP that made a request for content. The Edge Location Report shows the total number of traffic delivered through each edge location. Each report measures traffic in three ways: the total number of requests, the total number of bytes transferred, and the number of request broken

down by HTTP response code. The LogAnalyzer is implemented using Cascading (http://www.cascading.org) and is an example of how to construct an Amazon Elastic MapReduce application. Customers can also customize reports generated by the LogAnalyzer.

6.6.3 SERVICENOW

The ServiceNow application writes detailed log information that is stored in tables within a customer's instance. As this is customer data in a customer's instance, ServiceNow does not attempt to monitor or view this data unless specifically requested by a customer. As a result, the customer is responsible for monitoring the contents of these logs files. The log data is protected in the same manner as all other customer data. Event logs can also be configured to feed into a customer's environment via ServiceNow's Syslog probe allowing the logs to be stored within the customer's environment in a syslog repository or SIEM and retained according to the customer's requirements.

ServiceNow's application logging includes verbose transaction logs, these logs are retained within the instance for 30 days. Event logs are stored for seven days and audit histories are retained indefinitely in the instance.

Transaction logs represent every click, view, and system event that occurs in an instance and as a result, will grow very large, quickly. They provide a level of detail that is frequently used for troubleshooting issues with an instance. They can also provide detailed intelligence on the behaviors within an instance. These logs can be downloaded to customers' environments, if they need to be retained for longer than 30 days.

The event logs on the other hand are less granular; they will include the creation of an incident, or deletion of problem, or any one of the 250 standard events. They may also contain customer created events. There are a number of security events as well, including successful login, failed login, security privilege escalation, and viewing of a table. These events can either be monitored manually, generate an Incident based on a parameter or when metric is reached; such as failed logins per minute.

The final aspect of logging is the audit history. Audit history may be turned on for any particular table or field. The audit log table then maintains a record of who made changes when to a table or field and what they changed.

6.7 Restrict Visibility (8.6.7)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

Each of our proposed CSPs provide Identity and Access Management (IAM) solutions that, when properly implemented, satisfy their customers' mission-critical needs to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements.

6.7.1 APPDYNAMICS

AppDynamics includes an extensive built in Role Based Access Control (RBAC) whereby you as an administrator have control over who can see what data and who can make configuration changes to the system. After you install AppDynamics you can add user accounts in the Controller UI, allowing other users to access the UI and configure AppDynamics. The Account Owner is the predefined role with the Administer users, groups, roles permission.

The Controller can authenticate users against local user accounts or against external LDAP or SAML-based authentication providers. A user can belong to one or more groups. Groups let you assign and manage roles for users collectively. Roles are an important concept in the Controller UI. Roles determine what users can see or do in the UI, including which business applications they can monitor and the types of configuration changes they can make. Parts of the UI are not visible to users whose roles do not authorize access to those features. A user or group can have more than one role, but should have at least one.

AppDynamics comes with a set of predefined roles, but you can add your own, particularly to set up user access by business application

☑ *For more information beyond this requirement, visit online documentation at https://docs.appdynamics.com/display/PRO44/Manage+Users+and+Groups*

6.7.2 AWS

AWS Identity and Access Management (IAM) enables customers to securely control access to AWS services and resources for their users. Using IAM, customers can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources. IAM allows you to:

- Manage IAM users and their access – You can create users in IAM, assign them individual security credentials (i.e., access keys, passwords, and multi-factor authentication devices) or request temporary security credentials to provide users access to AWS services and resources. You can manage permissions in order to control which operations a user can perform.
- Manage IAM roles and their permissions – You can create roles in IAM, and manage permissions to control which operations can be performed by the entity, or AWS service, that assumes the role. You can also define which entity is allowed to assume the role.
- Manage federated users and their permissions – You can enable identity federation to allow existing identities (e.g., users) in your enterprise to access the AWS Management Console, to call AWS APIs, and to access resources, without the need to create an IAM user for each identity.

6.7.3 SERVICENOW

ServiceNow includes built in Role Based Access Control (RBAC) that is based on users, groups and roles. The entitlements granted to users are built from fine grained Access Control Lists (ACLs). ACLs can be built from individual entitlements that include read, write, create, execute and delete as well as a number of other individual attributes. The attributes that are available also vary, depending on the type of object being secured. Customers have full control of the entitlements granted to each of their users and integration with customer side directory service is possible through the use of users, groups and group memberships.

6.8 Notification Process (8.6.8)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

Red River has described its notification process in the event of a security incident for each vendor below.

6.8.1 APPDYNAMICS

☑ *Please see Section 3.1 Data Breach (8.3.1) Subsection 3.1.1 AppDynamics and Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018) for notification process information*

6.8.2 AWS

AWS has implemented various methods of external communication to support its customer base and the community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.

☑ *Please refer to AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

6.8.3 SERVICENOW

ServiceNow has multiple methods of communication as part of our expansive customer service support and incident response processes.

☑ *Please see Section 3.1 Data Breach (8.3.1) Subsection 3.1.3 ServiceNow and Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018) beginning on page 217 for more information on notification processes*

6.9 Security Controls (8.6.9)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

6.9.1 AppDynamics

AppDynamics SaaS offering that uses industry-standard multi-tenancy controls to ensure the confidentiality of customers' data in a multi-tenant environment. The AppDynamics SaaS platform (servers, infrastructure and storage) is hosted in one of the largest Tier III data centers in North America. The data center is designed and constructed to deliver world-class physical security, power availability, infrastructure flexibility, and growth capacity. The data center provider is SSAE 16 SOC 1 Type II compliant, which means that it has been fully independently audited to verify the validity and functionality of its control activities and processes.

Every server is operated in a fully redundant fail-over pair to ensure high availability. Data is backed up nightly, stored redundantly and can be restored rapidly in case of failure. Security updates and patches are actively evaluated by engineers and are deployed based upon the security risks and stability benefits they offer to the AppDynamics SaaS platform and customers.

6.9.2 AWS

The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI QSA and was found to be in compliance with all requirements of PCI DSS version 3.2 published in April 2016. More information on AWS's multi-tenant architecture is found in the *AWS Risk and Compliance* whitepaper.

AWS also has single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within your Amazon Virtual Private Cloud (Amazon VPC) that run hardware dedicated to a single customer. Dedicated Instances let you take full advantage of the benefits of Amazon VPC and the AWS Cloud while isolating your Amazon EC2 compute instances at the hardware level. AWS isolation and deployment options are illustrated below.

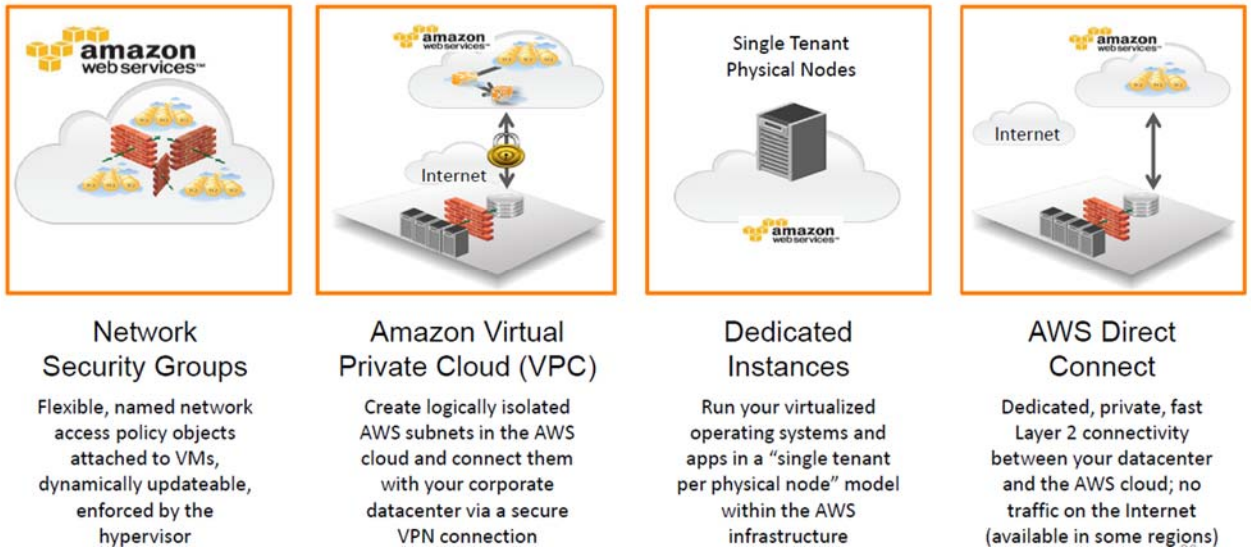


Figure 4: AWS Isolation and Deployment Options

6.9.3 SERVICENOW

ServiceNow's architecture is built on a ServiceNow fully owned operated private cloud. This private cloud hosts the ServiceNow platform and applications that are offered to its customers under a subscription service model. The ServiceNow private cloud operates out of colocation data centers that provide robust physical and environmental controls, with ServiceNow staff exclusively providing the logical management. Access to the private cloud where customer data is hosted is only granted to ServiceNow staff based on their roles and job requirements. ServiceNow does not outsource any function that would give a third-party access to customer data. ServiceNow's private cloud is a highly standardized environment from the identically configured cages in the data centers through to the consistent logical infrastructure.

This private cloud is home to just ServiceNow, limiting the private cloud's footprint to only those technologies required to support this service. This allows for highly restricted networking rule sets regarding ingress and egress requirements and facilitates the ability for hardened systems, only allowing for the small number of necessary services, protocols and ports to be enabled. A ServiceNow instance represents an isolated logical environment consisting of application nodes in the web application tier and a dedicated database. Each customer will receive at least two instances, a production High Availability (HA) instance and a sub-production instance without HA.

Each instance is accessed via a unique Domain name in the form of customername.servicenow.com' (for a production instance) and 'customername-dev.service-now.com' as a sub-production example. There is no comingling of any customer data between instances and there is no single shared multi-tenant databases, with data from multiple customers stored therein.

6.10 Security Technical Reference Architectures (8.6.10)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

Red River has verified that the proposed CSPs have developed and maintain secure, scalable and cost-efficient cloud solutions – and we provide the Path to Cloud framework to work collaboratively with clients and CSRs to transition legacy operations to the cloud (e.g., "Life and shift") and establish new cloud solutions.

6.10.1 AppDynamics

AppDynamics provides an overview of its SaaS architecture in its SOC 2 report, which will be provided to potential clients under NDA. AppDynamics does not provide IaaS or PaaS.

6.10.2 AWS

The following whitepapers may prove helpful in your formulation of a response to these questions.

- *Architecting for the Cloud: AWS Best Practices (February 2016)* contains prescriptive guidance for architects designing solutions with AWS services. *https://d1.awsstatic.com/whitepapers/AWS_Cloud_Best_Practices.pdf*
- *Managing Your AWS Infrastructure at Scale Feb 2015* contains information on tools and techniques for managing your AWS environment at any scale. https://d0.awsstatic.com/whitepapers/managing-your-aws-infrastructure-at-scale.pdf
- Additional whitepapers are located at: https://aws.amazon.com/whitepapers/

6.10.3 ServiceNow

The ServiceNow global security team is focused on protecting the confidentiality, integrity, privacy, and availability of the data and the services we deliver. It performs the functions listed in the diagram below.

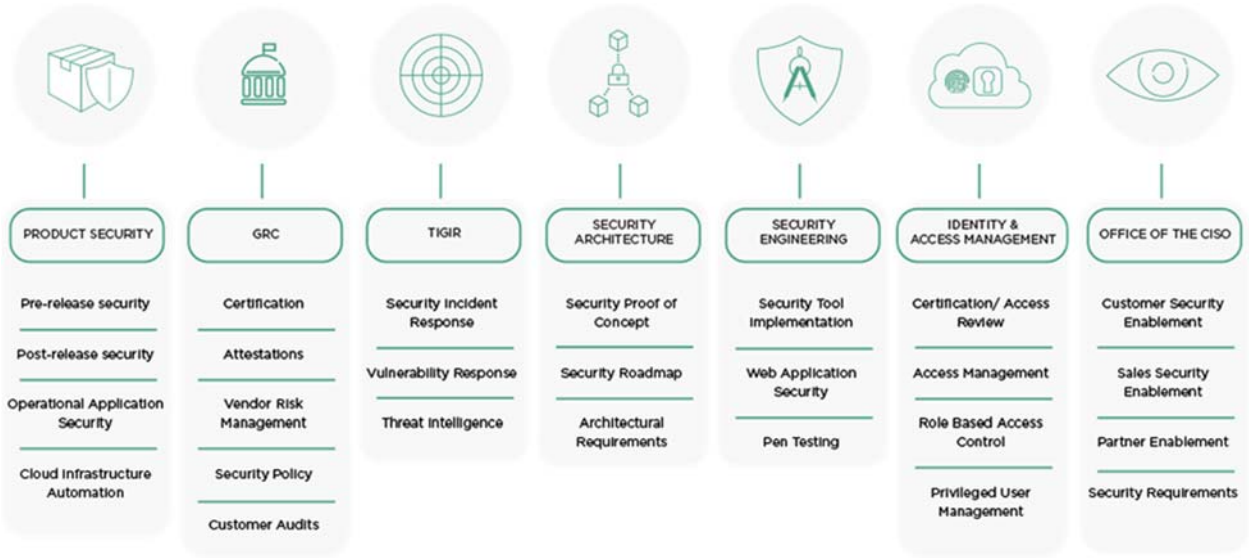


Figure 5: ServiceNow Security Framework

- Physical Security - Physical security begins with the global co-location data centers at which the service is hosted. The ServiceNow data centers are highly secure facilities with 24x7x365 security guards, CCTV, multiple levels of entry controls, and strict procedures for physically entering the facility. Within each data center, all ServiceNow equipment is stored in one or more dedicated, anonymous ServiceNow co-location spaces. The cages are further protected behind biometric access controlled doors. And all ServiceNow data center providers must be either ISO/IEC 27001:2013 accredited and/ or produce regular SSAE 16 Type 2 attestations.
- Cloud Security – customer instances are hosted in our SaaS environment. We refer to it as “private” because the environment is dedicated to only hosting our subscription service and no other public cloud hosting capabilities are used to deliver the service.
- Host Security – The protection of the host starts with the use of a hardened open source operating system that is regularly patched using automated configuration management. Comprehensive vulnerability response processes scan all hosts daily and they are patched regularly to meet compliance mandates
- DDoS Protection - ServiceNow takes the threat of Distributed Denial of Service (DDoS) very seriously and has deployed a multi-tiered defense system that continually monitors for attacks and mitigates them. DDoS attack traffic is identified and discarded at the edge of our cloud. This allows customers to maintain access to their instances even during an attack.
- Logical Security - we have implemented specific logical security zones. These zones are logically separated and protected using logical access controls as highlighted in Figure 6: ServiceNow Layered Security Model.

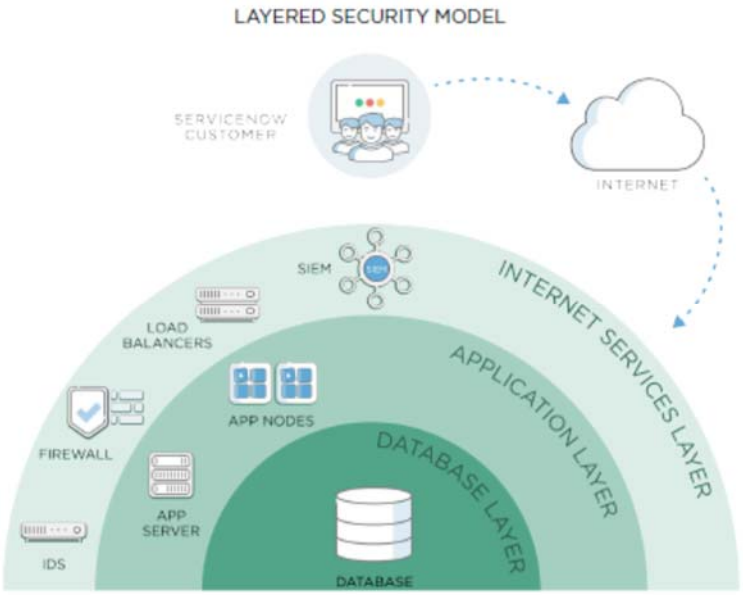


Figure 6: ServiceNow Layered Security Model

ServiceNow provides an overview of its SaaS architecture in its SOC report, which will be provided to potential clients under NDA.

☑ *Please see ServiceNow technical reference architecture documentation at https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/ebook/ebk-how-servicenow-delivers-safe-and-secure-cloud-services.pdf for extensive detail*

6.11 Employee Security Procedures (8.6.11)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

Red River requires applicants to undergo a series of steps prior to being made an offer of employment. This includes a completed job application, right to work documentation, background investigation, and employment history. As a standard practice, Red River conducts pre-hire background checks on all new employees. Background checks are performed after the candidate accepts an offer with us and prior to their official employment start date.

The background checks typically include the following:

- Social Security Address Trace
- National Criminal History with Alias Search
- Terrorist Watch List

- County Criminal History
- Unlimited County Criminal History (7 year)
- Address to Statewide Criminal History (7 year)
- Special Review Process – employment and/or education history
- FACIS Level 3 (OIG, GSA, DEA, EPLS, FDA, PHS, ORI, Tric)
- TS SCI for Federal or Specialized contracts

Red river will conduct current background checks on any Red River or subcontractor personnel who work in an Entity owned/ leased/ rented facility, and provide proof and results of those background checks to the Entity.

6.11.1 AppDynamics

Pre-employment background checks are conducted on all job applicants who receive an offer of employment. AppDynamics personnel are employed by Cisco Systems, Inc. (Cisco), AppDynamics' parent company. Cisco uses a third-party agency to conduct background checks to verify the accuracy of the information provided by the applicant during the selection process. Cisco complies with all applicable federal, state and local laws, including fair employment practices and equal employment opportunity, when conducting background checks. Offers of employment are conditional upon Cisco's receipt of a pre-employment background check that is acceptable to Cisco, at Cisco's sole discretion. Any applicant who refuses to complete the background check process will not be eligible for employment. The following checks are conducted as part of the pre-employment background check process:

(1) Criminal Conviction History, (2) Prohibited Parties, (3) Social Security Number (SSN) Trace (US only), (4) Previous Employment History, (5) Education Verification, (6) other screening as deemed appropriate by Cisco for the job role.

Furthermore, AppDynamics uses industry-standard techniques designed to restrict access to and to prevent unauthorized use of its Information Systems. AppDynamics requires the use of individual user accounts to maintain the integrity of audit trails. User and group management is centralized using single-sign-on systems and access to systems is subject to management approval. Access to sensitive systems, including all systems that process or store Customer Data is reviewed and re-approval is required periodically.

6.11.2 AWS

AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure and customers are responsible for securing the workloads they deploy in AWS. AWS has established formal policies and procedures to delineate the minimum standards for logical access to AWS platform and infrastructure hosts. AWS conducts pre-employment criminal background checks, as permitted by law, for employees commensurate with their position and level of access. The AWS SOC reports provides additional details regarding the controls in place for background verification.

6.11.3 SERVICENOW

ServiceNow conducts pre-employment criminal background checks, as permitted by law, for employees commensurate with their position and level of access. The ServiceNow SOC reports provides additional details regarding the controls in place for background verification.

6.12 Confidentiality of Data Types (8.6.12)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

Please refer to Section 9.1 Encryption Technologies [RFP 8.9.1] for more information on securing data at rest and in transit.

6.12.1 APPDYNAMICS

AppDynamics encrypts all customer data in transit and at rest using industry-standard encryption such as TLS 1.2 and AES 256. AppDynamics agents typically push data using one-way HTTP or HTTPS connections to a single host (a Controller) which has been allocated to one or more customer accounts. AppDynamics offers dedicated Controllers for customers who require their data to be isolated. For added security, agents can be configured to send data using encrypted transmission by simply selecting HTTPS port 443 and setting "controller-ssl-enabled" to true in the agent configuration. AppDynamics agents also have built-in support for outbound HTTP proxies for customers using these security mechanisms.

AppDynamics uses random staggering on agent data communication to the AppDynamics SaaS platform so traffic is spread evenly to minimize bursts and spikes of network traffic from the client data center to the AppDynamics SaaS platform.

6.12.2 AWS

AWS customers retain control and ownership of their data, and all data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. AWS offers the ability to add an additional layer of security to data at rest in the cloud by providing scalable and efficient encryption features. This includes:

- Data encryption capabilities in AWS storage and database services, such as Amazon EBS, Amazon S3, Amazon Glacier, Oracle RDS, SQL Server RDS, and Amazon Redshift.
- Flexible key management options, including AWS Key Management Service, that allow customers to choose whether to have AWS manage the encryption keys or keep complete control over their keys.
- Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing customers to satisfy compliance requirements.

- Support for both Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit.
- APIs for customers to integrate encryption and data protection with any of the services developed or deployed in an AWS environment.

The *AWS Security Best Practices* whitepaper provides greater detail on how to protect data in transit and at rest in the AWS Cloud. Other security resources are also available on our Cloud Security Resources page.

6.12.3 SERVICENOW

ServiceNow provides multiple methods of security adhering to NIST Standards, including such data in-flight encryption whereby as a ServiceNow customer, browser-based sessions to your ServiceNow cloud instance(s) are encrypted over the internet via Transport Layer Security (TLS) using AES-128 or AES-256 block ciphers and all end-user access to a ServiceNow instance is always automatically redirected to HTTPS if attempted over HTTP. ServiceNow can apply encryption to integrations, such as LDAP and Web Services, as well as commonly used file transfer methods. In the case of an LDAPS over SSL connection, you can conveniently store certificates for specific LDAP servers within a ServiceNow instance for use in signing instance-bound Web Service requests. We also support certificate-based mutual Web Services security authentication with external endpoints for all ServiceNow instances. Data can be securely transferred to your ServiceNow instances using pre-defined file transfer integration methods. You can also use clear text protocols such as FTP or HTTP to transfer data or support specific tasks, such as an approval or status request.

ServiceNow Encryption-at-rest security methods include Column level encryption, including support for AES-128, AES-256, and 3DES encryption algorithms, which can apply your choice to encrypt data. To mitigate the possible compromise of encrypted customer data, we re-encrypt (wrap) your keys with a secondary key. With Edge Encryption, unencrypted target data is never stored in your ServiceNow instance. It provides you with the capability for automatic key rotation. It supports tokenization and substitution of data, such as credit card or social security numbers, to match standard data structures. Full Disk Encryption allows for everything inside the co-location spaces are owned, operated, and managed by ServiceNow. This includes the management of hard drives and server hardware. All hard drives are sanitized prior to leaving our private cages (per NIST 800-88 guidelines) which ensures your data is appropriately handled and protected. You can choose to further mitigate data exposure caused by the loss or theft of storage devices with AES-256 full-disk encryption of your data at rest.

6.13 Data Breach Notification (8.6.13)

Utah Solicitation Number SK18008 Requirement: Page 27
8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

6.13.1 APPDYNAMICS

AppDynamics maintains an Incident Response Policy and trains all personnel identified in the policy of their responsibilities on a semi-annual basis. In the event of a suspected incident the incident response team is notified and immediately begins a reasonable investigation as to whether or not a breach has occurred. In the event of a reasonably suspected breach, AppDynamics will use commercially reasonable efforts to contain, mitigate, and resolve the breach as well as put in place additional controls to prevent further breaches of a similar type.

AppDynamics has retained a leading incident response provider to provide additional incident response capabilities and reserves the right to engage their services without prior approval from affected customers.

Notification - Where allowed by applicable law, AppDynamics will promptly notify affected customers of a security incident that affects Customer Data. Once AppDynamics has reasonably determined that Customer Data has been impacted, AppDynamics will promptly notify the impacted customer(s) following such determination. In accordance with its Incident Response Policy, AppDynamics will provide reasonable details regarding the incident, the steps taken by AppDynamics to contain, mitigate, resolve, and prevent future incidents provided that, in AppDynamics' sole discretion, such information does not impact the confidentiality of other AppDynamics customers or the overall security posture of AppDynamics.

☑ *Please refer to Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018) beginning on 141 for additional information on notification and response time expectations*

6.13.2 AWS

AWS Customers retain the responsibility to monitor their own environment for privacy breaches.

☑ *Please also see our response in Section 3.1 Data Breach (8.3.1) Subsection 3.1.2 AWS on page 2*

☑ *Please refer to AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

6.13.3 SERVICENOW

In the event of a confirmed Data Breach of customer data supplied to ServiceNow, ServiceNow will immediately notify the Red River Contract Manager, Phillip Wieser and he will then notify the customer. ServiceNow shall take reasonable measures to promptly mitigate the cause of the Breach and shall take reasonable corrective measures to prevent future Breaches. As information is collected or otherwise becomes available to ServiceNow and unless prohibited by law, ServiceNow shall provide information regarding the nature and consequences of the Breach that are reasonably requested to allow Customer to notify affected individuals, government agencies and/or credit bureaus. Customer is solely responsible for determining whether to notify impacted

Data Subjects and for providing such notice, and for determining if regulatory bodies or enforcement commissions applicable to Customer or Customer Data need to be notified of a Breach. These procedures are outline in our DPA and DSG which has been updated to meet the GDPR mandates.

☑ *Please see Section 3.1 Data Breach (8.3.1) Subsection 3.1.3 ServiceNow for detail on data breach notification processes*

☑ *Please see Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018) beginning on page 217 for more information on SLAs*

7. (E) MIGRATION AND REDEPLOYMENT PLAN (8.7)

7.1 Closing Down a Service (8.7.1)

Utah Solicitation Number SK18008 Requirement: Page 28
8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

Red River and CSPs will work collaboratively with the client to understand and apply the appropriate procedures. Red River's corporate and client engagements – and each of our proposed CSPs – maintain policies and procedures for function decommissioning, including:

- Immediate or Anniversary Date Cancellations - due to the number of offerings, customers are advised to understand the termination provisions in the service contract.
- Hard drives are decommissioned compliant with DOD 5220.22-M or NIST 800-88. This process is monitored and logged to provide an auditable history of any drive.

Our experience indicates client responsibilities include, but may not be limited to

- Backing up any applications and data they wish to retain prior to closing and account or cancelling a device.
- Deleting existing applications and associated data to avoid any future consumption charges.
- Any charges accrued during the billing cycle.
- Reviewing the terms and conditions of the service, especially with respect to customer data, and understanding what sections survive the termination of an agreement.

7.1.1 APPDYNAMICS

AppDynamics provides access to all data stored in the platform via REST API during the lifetime of the agreement. Due to the proprietary nature of the platform, AppDynamics does not provide migration services to other vendors. AppDynamics' media sanitization and data destruction policies and procedures are aligned with NIST SP 800-88.

7.1.2 AWS

AWS Customers manage the creation and deletion of their data on AWS, as well as maintain control of access permissions. Customers are responsible for maintaining appropriate data retention policies and procedures. Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data is and server instances are logically isolated from other customers by default. Privileged user access control is

reviewed by an independent auditor during the AWS SOC 1, ISO 27001, PCI, and FedRAMP audits. Refer to the AWS SOC 1 audit report (available under AWS NDA) for more information and validation of the control testing related to access permissions and data deletion for AWS S3 Services. Refer to the AWS PCI Compliance Package (available under AWS NDA) for testing performed to confirm data deletion. Both the AWS SOC 1 audit report and the AWS PCI Compliance Package can be requested at **http://aws.amazon.com/compliance/contact/**.

7.1.3 SERVICENOW

ServiceNow believes in the shared responsibility model and as a ServiceNow customer, you have control over the security of your instance and your data within the ServiceNow cloud services. A single data classification is applied to all customer data we host. We do not inspect or monitor the data. As our customer, you apply access controls to restrict access within your instances based on your requirements and needs, in accordance with your data classification policies.

The ServiceNow client decides what information is to be stored, how it is to be used, and how long it is retained. All your data is hosted on solid-state or mechanical disks within our co-location spaces. No tapes or other forms of removable media are used to provide the service, including for backups. When functional storage devices reach their end-of life or get reassigned to new customers, they are shredded based on guidance from NIST.

Throughout the lifetime of your subscription, your data can be directly exported from the ServiceNow instance. This can be via the UI, through integrations, or by using other ServiceNow components. We return all your data in an SQL dump format at the end of a contract. All hosted backed-up data is automatically deleted and overwritten 45 days from the end of a contract.

7.2 Return of Data (8.7.2)

Utah Solicitation Number SK18008 Requirement: Page 28
8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

Red River has provided CSP-specific responses below.

7.2.1 APPDYNAMICS

☑ *Please see our response to Section 7.1 Closing Down a Service (8.7.1) Subsection 7.1.1 AppDynamics above*

7.2.2 AWS

☑ *Please see our response to Section 7.1 Closing Down a Service (8.7.1) Subsection 7.1.2 AWS above*

7.2.3 SERVICENOW

☑ *Please see our response to Section 7.1 Closing Down a Service (8.7.1) Subsection 7.1.2 ServiceNow*

8. (E) SERVICE OR DATA RECOVERY (8.8)

8.1 Service or Data Recovery Steps (8.8.1)

Utah Solicitation Number SK18008 Requirement: Page 28

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.

- *a. Extended downtime.*
- *b. Suffers an unrecoverable loss of data.*
- *c. Offeror experiences a system failure.*
- *d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.*
- *e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).*

Red River will work with clients to define and document expectations for scheduled and unscheduled downtime events. In the event of extended downtime for any reason, Red River and the CSP will utilize existing escalation and notification policies collaboratively developed to communicate timelines and expectations. Should an unrecoverable loss of data occur, Red River and CSPs will leverage snapshots and automated restore processes to return the impacted instances and services to a working state. If upon investigation of the data loss is unrecoverable, is at fault for failing to meet an SLA or has failed to follow the mutually-agreed Backup/DR policy, service credit will be awarded based on severity of data loss and SLA.

Red River will work with clients to verify costs and benefits of a tailored DR plan that meets the requirements of the specific environment.

8.1.1 AppDynamics

AppDynamics maintains infrastructure to provide online services for “around the clock” production operations (24x7x365), as well as disaster recovery. The disaster recovery infrastructure is designed to be able to take over 100% of the AppDynamics service in case of primary infrastructure failure, referred to as a disaster throughout the remainder of this document. AppDynamics has built infrastructure in place to meet the following recovery objectives:

- Recovery point objective (RPO): 24 hours
- Recovery time objective (RTO): 72 hours

In the case of a disaster, this equates to a commitment that the AppDynamics service will not be down for longer than 72 hours and will not lose more than 24+72 hours of data.

Figure 7: AppDynamics Disaster Process

AppDynamics has implemented a number of processes and technologies in order to provide business continuity and consistently maintain recovery objectives.

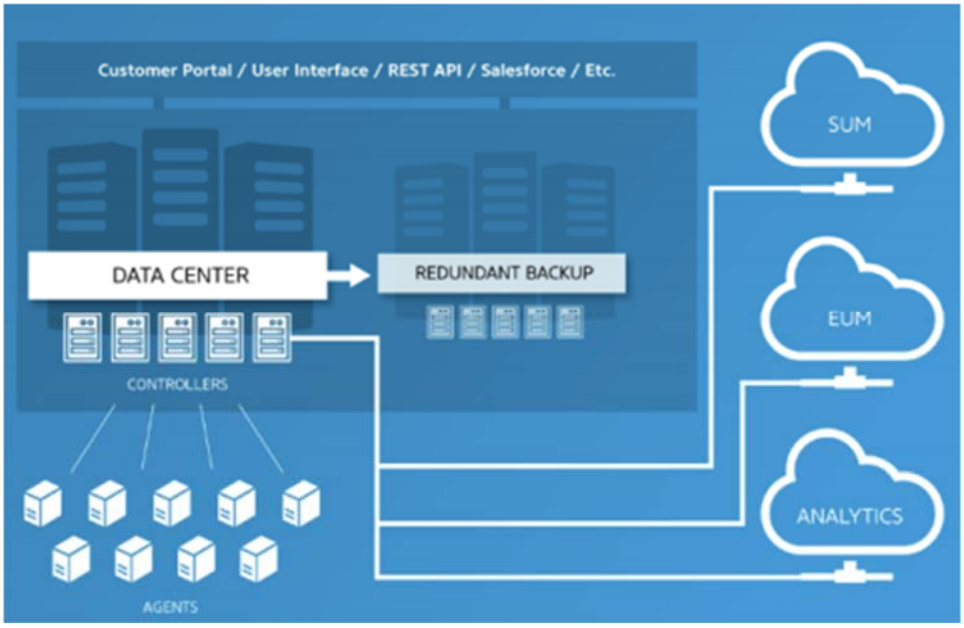


Figure 8: AppDynamics Network Diagram

AppDynamics deploys infrastructure in fully redundant pairs to minimize single points of failure. This ensures that a failure of any single hardware component does not compromise the availability of production services.

Critical systems and application data required for disaster recovery are replicated from AppDynamics' Chicago Datacenter to the San Francisco Datacenter over a 10Gb/s network connection. Data is backed up once a day locally in Chicago, and is transferred to San Francisco every 24 hours. Data is stored on a storage server in a secure network zone within the San Francisco datacenter. Testing is done to ensure the disaster recovery environments are up to date and critical synchronization mechanisms are functioning properly.

8.1.2 AWS

Amazon's infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. Data center Business Continuity Management at AWS is under the direction of the Amazon Infrastructure Group.

8.1.2.1 Availability

Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS provides you with the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

You should architect your AWS usage to take advantage of multiple regions and availability zones. Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure modes, including natural disasters or system failures.

8.1.2.2 Fault-Tolerant Design

Amazon's infrastructure has a high level of availability and provides you with the capability to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact.

Data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS provides you with the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region). In addition to utilizing discrete uninterruptable power supply (UPS) and onsite backup generators, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

You should architect your AWS usage to take advantage of multiple regions and availability zones. Distributing applications across multiple availability zones provides the ability to remain resilient in the face of most failure scenarios, including natural disasters or system failures.

However, you should be aware of location-dependent privacy and compliance requirements, such as the EU Data Privacy Directive. Data is not replicated between regions unless proactively done so by the customer, thus allowing customers with these types of data placement and privacy requirements the ability to establish compliant environments. It should be noted that all communications between regions is across public Internet infrastructure; therefore, appropriate encryption methods should be used to protect sensitive data.

As of this writing, AWS currently has 18 regions, 54 Availability Zones, and 1 Local Region throughout the world: US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-West), Canada (Central), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Osaka-Local), South America (Sao Paulo), China (Beijing), and China (Ningxia). Information on each region can be found at the AWS Global Infrastructure webpage.

AWS GovCloud (US) is an isolated AWS Region designed to allow US government agencies and customers to move workloads into the cloud by helping them meet certain regulatory and compliance requirements. The AWS GovCloud (US) framework allows US government agencies and their contractors to comply with U.S. International Traffic in Arms Regulations (ITAR) regulations as well as the Federal Risk and Authorization Management Program (FedRAMP) requirements. AWS GovCloud (US) has received an Agency Authorization to Operate (ATO) from the US Department of Health and Human Services (HHS) utilizing a FedRAMP accredited Third-Party Assessment Organization (3PAO) for several AWS services.

The AWS GovCloud (US) Region provides the same fault-tolerant design as other regions, with two Availability Zones. In addition, the AWS GovCloud (US) region is a mandatory AWS Virtual Private Cloud (VPC) service by default to create an isolated portion of the AWS cloud and launch Amazon EC2 instances that have private (RFC 1918) addresses. More information about GovCloud is available on the AWS website: http://aws.amazon.com/govcloud-us/

8.1.3 SERVICENOW

ServiceNow's data centers and cloud-based infrastructure have been designed to be highly available. All servers and network devices have redundant components and multiple network paths to avoid single points of failure. At the heart of this architecture, each customer application instance is supported by a multi-homed network configuration with multiple connections to the Internet. Production application servers are load balanced within each data center. Production database servers are replicated in near-real time to a peer data center within the same geographic region. ServiceNow leverages this Advanced High Availability (AHA) architecture for customer production instances in several ways:

- In the event of the failure of one or more infrastructure components, service is restored by transferring the operation of customer instances associated with the failed components to the peer data center.

- Before executing required maintenance, ServiceNow can proactively transfer operation of customer instances impacted by the maintenance to the peer data center. The maintenance can then proceed without impacting service availability. This approach means that the transfer between active and standby data centers is being regularly executed as part of standard operating procedures – ensuring that when it is needed to address a failure, the transfer will be successful and service disruption minimized.

For disasters that could impact an entire data center, ServiceNow maintains comprehensive disaster recovery, business continuity, and information system contingency plans that cover our production environments.

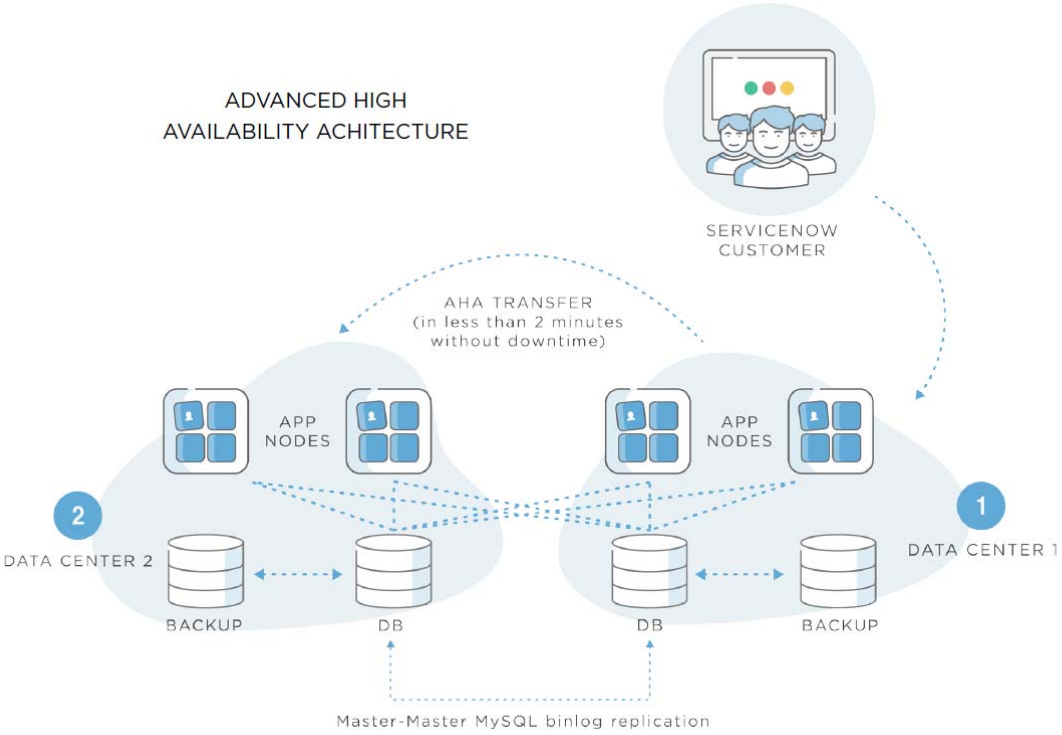


Figure 9: ServiceNow Architecture

8.2 Backup and Restore Services (8.8.2)

Utah Solicitation Number SK18008 Requirement: Page 28
8.8.2 Describe your methodologies for the following backup and restore services:
a. Method of data backups
b. Method of server image backups
c. Digital location of backup storage (secondary storage, tape, etc.)
d. Alternate data center strategies for primary data centers within the continental United States.

Red River has provided CSP-specific responses below.

8.2.1 APPDYNAMICS

AppDynamics has designed its SaaS architecture with fault tolerance in mind and leverages the multi-availability zone and multi-region capabilities of Amazon Web Services. In addition, AppDynamics leverages AWS' tools for snapshot, backup, and restore of individual services to other AWS regions and or services.

☑ *Please see our response to Section 8.1 Service or Data Recovery Steps (8.8.1) Subsection 8.1.1 AppDynamics above*

8.2.2 AWS

☑ *Please see our response to Section 8.1 Service or Data Recovery Steps (8.8.1) Subsection 8.1.2 AWS above*

8.2.3 SERVICENOW

☑ *Please see our response to Section 8.1 Service or Data Recovery Steps (8.8.1) Subsection 8.1.2 ServiceNow*

9. (E) DATA PROTECTION (8.9)

9.1 Protecting Data (8.9.1)

Utah Solicitation Number SK18008 Requirement: Page 28
8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

Each of our proposed CSPs provide standard encryption technologies and options to protect sensitive data while in transit or at rest.

9.1.1 APPDYNAMICS

AppDynamics is committed to providing strong levels of security assurance for our customers, our partners, and our community. Through the development of our cross-functional security program, our employees are working hard to ensure the security of our software products and services and our systems that we leverage to operate our company.

Our goal is to ensure continuous protection that meets and even exceeds industry standards for confidentiality, integrity, and availability of the data entrusted to us by our customers. Our program has been externally reviewed for SOC 2 compliance and we continue to adapt to remain agile to new and evolving threats facing our customers and our company.

To provide customers with transparency and assurance about its security program AppDynamics undergoes semi-annual SOC 2 Type II audits according the guidelines established by AICPA in AT Section 101 and TSP Section 100. AppDynamics has developed model clauses consistent with the EU Data Protection Directive 95/46/EC that cover the transfer of personal information outside of the European Economic Area (EEA). AppDynamics utilizes SSL certificates issued by DigiCert, Inc. and all endpoints support SSL/TLS encryption.

☑ *Please see our response to Section 31 APPENDIX: AppDynamics Security and Privacy Standard - CONFIDENTIAL beginning on page 243 for a complete listing of the AppDynamics data protection elements*

9.1.2 AWS

There are several options for encrypting data at rest, ranging from completely automated AWS encryption solutions (such as AWS Key Management Service [KMS]) to manual, client-side options (such as AWS CloudHSM). Choosing the right solutions depends on which AWS Cloud services are being used and customer requirements for key management. Information on protecting data at rest using encryption can be found in the Protecting Data Using Encryption section of the Amazon Simple Storage Service (Amazon S3) Developer Guide.

Additionally, the *Encrypting Data at Rest* whitepaper provides an overview of the options for encrypting data at rest in AWS Cloud services. It describes these options in terms of where

encryption keys are stored and how access to those keys is controlled. Both server-side and client-side encryption methods are discussed with examples of how each can be accomplished in various AWS Cloud services.

9.1.2.1 Securing Data in Transit

Protecting data in transit when running applications in the cloud involves protecting network traffic between clients and servers and network traffic between servers.

Services from AWS provide support for both Internet Protocol Security (IPSec) and Secure Sockets Layer/Transport Layer Security (SSL/TLS) for protection of data in transit. IPSec is a protocol that extends the IP protocol stack, often in network infrastructure, and allows applications on upper layers to communicate securely without modification. SSL/TLS, on the other hand, operates at the session layer, and while there are third-party SSL/TLS wrappers, it often requires support at the application layer as well.

The *AWS Security Best Practices* whitepaper provides greater detail on how to protect data in transit and at rest in the AWS Cloud.

9.1.3 SERVICENOW

ServiceNow makes use of encryption for both data in transit and data at rest aligning with industry standards and best practices.

☑ *Please see our response in Section 5.1 Protecting Data (8.5.1) Subsection 5.1.3 ServiceNow for detail on data protection standards and processes*

9.2 Business Associate Agreement (8.9.2)

Utah Solicitation Number SK18008 Requirement: Page 28
8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

Upon award and request from a Purchasing Entity, Red River would be willing to sign Business Associate Agreements or similar agreements that are set forth with a purpose of protecting customer data.

9.2.1 APPDYNAMICS

Generally, AppDynamics' Legal, Security, and Privacy teams are willing and able to review supplemental terms and/or agreements that are relevant to the data collection and processing done by the AppDynamics SaaS software. AppDynamics does not sign Business Associate Agreements (as defined under HIPAA/HITECH) because AppDynamics' products are not designed to collect or process PHI and therefore AppDynamics is not HIPAA certified and does not represent that it has such capability or certification set out in a BAA. AppDynamics products are not intended to process, store, transmit, or otherwise access personal health information or

personally identifiable information and as such AppDynamics does not meet the definition of a Business Associate or Covered Entity under the HIPAA Rules.

For the avoidance of doubt, the AppDynamics EULA for its SaaS software prohibits the sending of such information to AppDynamics' SaaS environment. However, AppDynamics' software could potentially be configured to collect parameter data, which may include personal health information depending on how the customer's application uses parameter data. By default, AppDynamics' software does not collect payload or parameter information.

AppDynamics can offer an on-premises solution for customers who wish to maintain full control over their deployment of the software. With this type of deployment, AppDynamics has no access to the software or the data it collects and processes (unless a customer manually sends that data through another out-of-band channel).

9.2.2 AWS

AWS has a standard Business Associate Addendum (BAA) we present to customers for signature. It takes into account the unique services AWS provides and accommodates the AWS Shared Responsibility Model.

9.2.3 SERVICENOW

Generally, ServiceNow is willing and able to review supplemental terms and/or agreements that are relevant to the data collection and processing done ServiceNow SaaS. ServiceNow does not sign Business Associate Agreements as ServiceNow does not access or view client data

9.3 Use of Data (8.9.3)

Utah Solicitation Number SK18008 Requirement: Page 28
8.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

Red River agrees that it will only use data for the purposes defined in the Master Agreement, participating addendums, or related SLAs. Red River will not sell, participate in data mining or otherwise distribute the government data or government related data. It further commits that any commitments made by Red River shall be binding upon any of its subcontractors including data mining, distribution, or resale of above said data.

9.3.1 APPDYNAMICS

AppDynamics' Legal, Security, and Privacy teams work regularly with Product and Engineering teams to ensure that processing and use of customer data is only for the purposes set out in the AppDynamics EULA. Our SOC 2 audit covers key controls that help ensure that access to and use of customer data is controlled, reasonably safeguarded using technical and organizational methods that meet or exceed industry standards. In addition, the Legal team includes appropriate contractual obligations and restrictions on subcontractor activity and processing to ensure compliance in this area.

☑ *The most current list of sub-processors is maintained at https://www.appdynamics.com/privacy/subprocessors/ and highlighted below*

- *AWS - AppDynamics leverages the Amazon Web Services (AWS) Virtual Private Cloud platform to host portions of its SaaS environment (global)*
- *Imperva Incapsula - AppDynamics leverages Incapsula to provide protection against distributed-denial-of-service (DDoS) attacks for its SaaS environment (global)*
- *IBM Softlayer - AppDynamics leverages IBM Softlayer to provide additional points-of-presence for its Synthetic User Monitoring product allowing customers to test their applications from additional geographic locations worldwide (global)*
- *Zendesk - AppDynamics leverages Zendesk's ticket management software-as-a-service platform to provide customer support (US)*

9.3.2 AWS

AWS does not access or use customer content for any purpose other than as legally required and to provide the AWS services selected by each customer, to that customer and its end users. AWS never uses customer content or derives information from it for other purposes such as marketing or advertising.

9.3.3 SERVICENOW

As a ServiceNow customer, you decide what information is to be stored, how it is to be used, and how long it is retained. ServiceNow does not use customer for purposes other than legally or contractually required by the customer.

☑ *Please see our response in Section 5.1 Protecting Data (8.5.1) Subsection 5.1.3 ServiceNow for detail on data protection standards and processes*

10. (E) SERVICE LEVEL AGREEMENTS (8.10)

10.1 Service Level Agreement Negotiations (8.10.1)

Utah Solicitation Number SK18008 Requirement: Page 27
8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

Red River has a long history of establishing clear and documented SLAs as well as the associated compliance monitoring tools and reporting. We initiate every potential engagement with a collaborative discussion on the areas and items that are non-negotiable from the CSP and areas where either the CSP and/or Red River can exercise alternative provisions.

In general, our experience is that CSPs do not negotiate terms of their standard SLAs. At the same time, we do have expertise in working with CSPs to identify and define unique scenarios, such as significant scale or highly specific requirements, where CSPs may have the flexibility to alter an SLA.

10.1.1 APPDYNAMICS

AppDynamics SLA is non-negotiable. As such, we have built in remedies for excessive downtime in order to ensure customer success and satisfaction. Availability is measured by the following formula: (n - y) *100 / n

- N = the total number of minutes in the given calendar quarter minus the exclusions
- Y = the total number of minutes in the given calendar quarter that the Controller is not accessible

In the event the availability of the Software falls below the SLA, AppDynamics will pay End User a service credit corresponding to the actual availability of the Software during the applicable calendar quarter (on pro-rated basis for annual or multi-year fees

☑ *Please refer to the following sections for additional information on SLAs*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.1 AppDynamics*
- *Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018)*

10.1.2 AWS

AWS has millions of active Customers and AWS offers the same portfolio of self-service, highly automated web services to its Customers on a one-to-many basis. Because of this, AWS cannot commit to keep the Services or SLAs the same for certain customers but improve or change them for others. AWS needs the right to make changes across its customer base, and is not able to offer you a custom notice period. AWS has been continually expanding its services to support virtually any cloud workload, and it now has more than 100 services that range from compute,

storage, networking, database, analytics, application services, deployment, management, developer, mobile, Internet of Things (IoT), Artificial Intelligence (AI), security, hybrid, and enterprise applications.

☑ *Please refer to the following sections for additional information on SLAs*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.2 AWS*
- *AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

10.1.3 SERVICENOW

ServiceNow's SLA is not negotiable. ServiceNow delivers the same level of world-class support to all customers as described in the "Subscription Service Guide" included with this response. ServiceNow's homogeneous private cloud environment where all applications are on a single platform offers ServiceNow a competitive advantage in being able to concentrate its efforts to make the customer's user experience the best possible. The ServiceNow environment is a private cloud, fully owned and operated by ServiceNow. ServiceNow's experience and understanding of its private cloud and the benefits provided by a consistent infrastructure and standardized processes allow it to provide a high level of security, availability, and performance in a cost effective and reliable manner.

☑ *Please refer to the following sections for additional information on SLAs*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.3 ServiceNow*
- *Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018)*

10.2 Service Level Agreement Sample (8.10.2)

Utah Solicitation Number SK18008 Requirement: Page 28
8.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

Red River has provided CSP-specific responses below.

10.2.1 APPDYNAMICS

☑ *Please refer to the following sections for additional information on SLAs*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.1 AppDynamics*
- *Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018)*

10.2.2 AWS

☑ *Please refer to the following sections for additional information on SLAs*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.2 AWS*
- *AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

10.2.3 SERVICENOW

☑ *Please refer to the following sections for additional information on SLAs*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.3 ServiceNow*
- *Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018)*

11. (E) DATA DISPOSAL (8.11)

11.1 Data Disposal Procedures (8.11.1)

Utah Solicitation Number SK18008 Requirement: Page 28
Specify your data disposal procedures and policies and destruction confirmation process.

Red River, and each of our proposed CSPs, maintain data disposal procedures and policies that comply with DOD 5220.22-M or NIST 800-88. NIST 800-88 provides an industry best practice decision flow that provide the placemat for sanitization decisions that are commensurate with the security categorization of the confidentiality of information contained on their media.

11.1.1 AppDynamics

Users have the ability to delete their data. The End User shall send AppDynamics the details of the relevant Data it wishes to be deleted. AppDynamics will effectively destroy all relevant Data along with any medium or document containing said Data within 14 days from receiving the End User's request if the End User has purchased a dedicated AppDynamics instance or within 365 days if the End User is on a shared instance. AppDynamics shall send the End User written confirmation thereof on written request.

☑ *Please also refer to Section 7(E) MIGRATION AND REDEPLOYMENT PLAN (8.7) subsection 7.1.1 AppDynamics for standards and expectations for data handling*

11.1.2 AWS

AWS provides customers with the ability to delete their data. AWS customers retain control and ownership of their data, and it is the customer's responsibility to manage their data. When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

☑ *Please also refer to Section 7(E) MIGRATION AND REDEPLOYMENT PLAN (8.7) subsection 7.1.2 AWS for standards and expectations for data handling*

11.1.3 ServiceNow

ServiceNow believes in the shared responsibility model and as a ServiceNow customer, you have control over the security of your instance and your data within the ServiceNow cloud services. A single data classification is applied to all customer data we host. We do not inspect or monitor

the data. As our customer, you apply access controls to restrict access within your instances based on your requirements and needs, in accordance with your data classification policies.

Throughout the lifetime of your subscription, your data can be directly exported from the ServiceNow instance. This can be via the UI, through integrations, or by using other ServiceNow components. We return all your data in an SQL dump format at the end of a contract. All hosted backed up data is automatically deleted and overwritten 45 days from the end of a contract.

☑ *Please also refer to Section 7(E) MIGRATION AND REDEPLOYMENT PLAN (8.7) subsection 7.1.3 ServiceNow for standards and expectations for data handling.*

12. (E) PERFORMANCE MEASURES AND REPORTING (8.12)

12.1 Reliability and Uptime (8.12.1)

Utah Solicitation Number SK18008 Requirement: Page 29
8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

Each of the proposed CSPs guarantees different levels of "uptime" and formulas to determine "availability" – please refer to Sections below for CSP-specific thresholds. Red River initiates any potential engagements with a collaborative discussion about the performance parameters of the underlying CSP, how those thresholds are calculated and how best to align them with client requirements and tracking.

12.1.1 AppDynamics

AppDynamics Availability SLA is 99.5%. The platform was designed in a High Available architecture.

☑ *Please refer to Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018) beginning on 141 for additional information on uptime expectations*

12.1.2 AWS

AWS takes extensive precautions to help ensure that we will remain fully operational, with no loss of service for our hosted applications. AWS replicates critical system components across multiple Availability Zones to ensure high availability both under normal circumstances and during disasters such as fires, tornadoes, or floods. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. Each AWS Availability Zone runs on its own independent infrastructure, engineered to be highly reliable so that even extreme disasters or weather events should only affect a single Availability Zone. The data centers' electrical power systems are designed to be fully redundant and maintainable without impact to operations. Common points of failure, such as generators, UPS units, and air conditioning, are not shared across Availability Zones.

At AWS, we plan for failure by maintaining contingency plans and regularly rehearsing our responses. In the words of Werner Vogels, Amazon's

How reliable is an application hosted by AWS?

In 2014, Nucleus Research surveyed 198 AWS customers that reported moving existing workloads from on-premises to AWS and found that they were able to reduce unplanned downtime by 32% (see Availability and Reliability in the Cloud: Amazon Web Services).

CTO: "Everything fails, all the time." We regularly perform preventative maintenance on our generators and UPS units to ensure that equipment is ready when needed. We also maintain a series of incident response plans covering both common and uncommon events, and update them regularly to incorporate lessons learned and prepare for emerging threats.

While AWS goes to great lengths to provide availability of the cloud, our customers share responsibility for ensuring availability within the cloud. These customers and others like them have succeeded because they designed for failure and have adopted best practices for high availability, such as taking advantage of multiple Availability Zones and configuring Auto Scaling groups to replace unhealthy instances. The *Building Fault-Tolerant Applications on AWS* whitepaper is a great introduction to achieving high availability in the cloud. In addition, the AWS Well-Architected Framework codifies the experiences of thousands of customers, helping customers assess and improve their cloud-based architectures and mitigate disruptions.

In addition, the AWS Architecture Center is designed to provide customers with the necessary guidance and application architecture best practices to build highly scalable and reliable applications in the AWS Cloud. These resources will help you understand the AWS Cloud, its services and features, and will provide architectural guidance for design and implementation of systems that run on the AWS infrastructure.

☑ *Please refer to AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

12.1.3 SERVICENOW

ServiceNow's Availability SLA is 99.8%, excluding Excused Downtime of up to two hours per month. This is achievable through the use of the AHA architecture that provides failover capabilities for maintenance and service disruptions to minimize downtime.

☑ *Please see Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018) beginning on page 217 for more information on SLAs*

12.2 Uptime (8.12.1)

Utah Solicitation Number SK18008 Requirement: Page 29 *8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.*

Red River has provided CSP-specific responses below.

12.2.1 APPDYNAMICS

☑ *Please refer to the following sections for SLAs information, including reliability and uptime expectations*

- *Section 12.1 Reliability and Uptime (8.12.1) Subsection 12.1.1 AppDynamics*

- *Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018) beginning on 141 for additional information on uptime expectations*

12.2.2 AWS

AWS far exceeds the Uptime Institute Tiering certification. Tiering aspects do not take into consideration the nature of the services of the cloud environment, and although the uptime institution tiering can be a great guide, it ultimately does not accurately map to a cloud service provider organization. AWS does not have a Certified Uptime Tiering level; however, we operate a data center environment using N+1 architecture. AWS offers SLAs for services such as Amazon EC2 and Amazon EBS at 99.95%, and Amazon S3 with an SLA of 99.9%. Our generator backup capabilities are detailed in our SOC Reports (as is our discussion regarding business continuity planning and N+1 architecture).

☑ *Please refer to the following sections for SLAs information, including reliability and uptime expectations*
- *Section 12.1 Reliability and Uptime (8.12.1) Subsection 12.1.2 AWS*
- *AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

12.2.3 SERVICENOW

☑ *Please refer to the following sections for SLAs information, including reliability and uptime expectations*
- *Section 12.1 Reliability and Uptime (8.12.1) Subsection 12.1.3 ServiceNow*
- *Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018) beginning on page 217 for more information on SLAs*

12.3 Support (8.12.3)

Utah Solicitation Number SK18008 Requirement: Page 29
8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

Red River has provided CSP-specific responses below.

12.3.1 APPDYNAMICS

AppDynamics will provide access to a ticketing system that will be available twenty-four (24) hours per day, seven (7) days per week. The ticketing system will be maintained by qualified support specialists, who shall use commercially reasonable efforts to provide technical support regarding the Software.

☑ *For a preview of the AppDynamics portal, please see https://www.appdynamics.com/support/*
☑ *Please refer to the following section for customer support expectations*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.1 AppDynamics*
- *Section 4.1 Excellent Customer Service (8.4.1) Subsection 4.1.1 AppDynamics*
- *Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018) beginning on 141 for additional information on support expectations*

12.3.2 AWS

☑ *Please refer to the following section for customer support expectations*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.2 AWS*
- *Section 4.1 Excellent Customer Service (8.4.1) Subsection 4.1.2 AWS*
- *AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

12.3.3 SERVICENOW

Customer Support is provided by ServiceNow 24 hours a day, 7 days a week, including all holidays. Customer may contact ServiceNow using one of the following means:

- Support Portal Customer may get login access to this self-service portal by contacting its ServiceNow administrator.
- Phone using one of the numbers at http://www.servicenow.com/support/contact-support.html.
- Single Point of Contact for Contract and Compliance – Phillip Weiser (see Red River Organization and Staffing document)

☑ *For a preview of the ServiceNow portal, please see https://hi.service-now.com/*
☑ *Please refer to the following section for customer support expectations*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.3 ServiceNow*
- *Section 4.1 Excellent Customer Service (8.4.1) Subsection 4.1.3 ServiceNow*
- *Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018) beginning on page 217 for more information on SLAs*

12.4 SLA Remedies (8.12.4)

Utah Solicitation Number SK18008 Requirement: Page 29 *8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.*

Red River has provided CSP-specific responses below.

12.4.1 APPDYNAMICS

AppDynamics shall respond to error tickets in accordance with the tables set forth below. AppDynamics will use reasonable means to repair the error and keep End User informed of progress. AppDynamics makes no representations as to when a full resolution of the error may be made.

☑ *Please refer to the following section for specific remedy provisions*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.1 AppDynamics*
- *Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018) beginning on page 141*

12.4.2 AWS

☑ *Please refer to the following section for specific remedy provisions*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.2 AWS*
- *AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

12.4.3 SERVICENOW

☑ *Please refer to the following section for specific remedy provisions*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.3 ServiceNow*
- *Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018) beginning on page 217*

12.5 Downtime (8.12.5)

Utah Solicitation Number SK18008 Requirement: Page 29
8.12.5 Describe the firm's procedures and schedules for any planned downtime.

Red River has provided CSP-specific responses below.

12.5.1 APPDYNAMICS

AppDynamics will notify clients within forty-eight (48) hours for standard maintenance windows and within twenty-four (24) hours for other non-standard emergency Maintenance.

☑ *Please refer to the following section for downtime expectations*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.1 AppDynamics*
- *Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018) beginning on page 141*

12.5.2 AWS

AWS does not require systems to be brought offline to perform regular maintenance and system patching, and AWS's own maintenance and system patching generally do not impact customers. There may be occasions when AWS might schedule a customer instance for a reboot for necessary maintenance, such as to apply updates that require a reboot. No action is required on the customer's part; we recommend that customers wait for the reboot to occur within its scheduled window. These scheduled events are not frequent and if a customer instance will be affected by a scheduled event, they will receive an email prior to the scheduled event with details about the event, as well as a start and end date. Customers can also view scheduled events for their instance(s) by using the Amazon EC2 Console, API, or CLI. AWS will communicate with customers, either via email, or through the AWS Service Health Dashboard if service use is likely to be adversely affected.

☑ *Please refer to the following section for downtime expectations*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.2 AWS*
- *Section 4.1 Excellent Customer Service (8.4.1) Subsection 4.1.2 AWS*
- *AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

12.5.3 SERVICENOW

ServiceNow notifies customers at least 10 days prior to scheduled maintenance for infrastructure network, hardware or software that might impact service. ServiceNow targets no more than two hours of downtime due to scheduled maintenance per month.

☑ *Please refer to the following section for specific downtime expectation*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.3 ServiceNow*
- *Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018) beginning on page 217*

12.6 Recovery Metrics Not Met (8.12.6)

Utah Solicitation Number SK18008 Requirement: Page 29
8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

Red River has provided CSP-specific responses below.

12.6.1 APPDYNAMICS

☑ *Please refer to the following section for specific remedy provisions*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.1 AppDynamics*
- *Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018) beginning on page 141*

12.6.2 AWS

☑ *Please refer to the following section for specific remedy provisions*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.2 AWS*
- *AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

12.6.3 SERVICENOW

☑ *Please refer to the following section for specific remedy provisions*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.3 ServiceNow*
- *Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018) beginning on page 217*

12.7 Performance Reports (8.12.7)

Utah Solicitation Number SK18008 Requirement: Page 29
8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

Red River has provided CSP-specific responses below.

12.7.1 APPDYNAMICS

Custom dashboards let you create and arrange widgets to give users a visual overview of the data of interest to them. Similarly reports capture AppDynamics data in PDF files that you can send to recipients. Reports can be automatically generated on a regular schedule or created on-demand as needed. Reports and dashboards are useful for getting a high-level overview of the health and performance of your system on a regular basis.

12.7.1.1 Virtual War Room

AppDynamics provides a truly unique capability to establish a “virtual war room” to integrate a real-time dashboard with collaborative troubleshooting in the form of a focused chat room called "War Room Notes". As participants troubleshoot issues, they can add notes and data that are visible to other participants. The notes display in a timeline format and are visible to all war room participants immediately as they are posted.

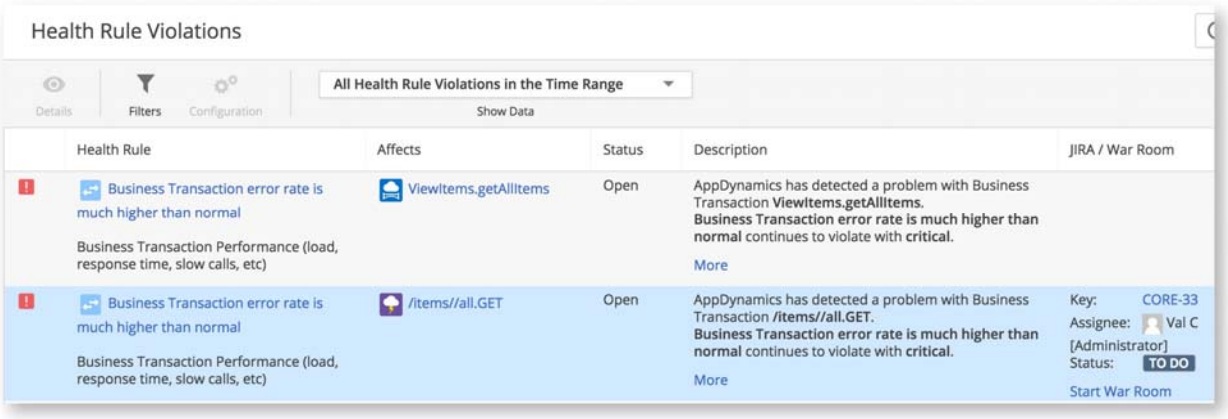


Figure 10: AppDynamics Virtual War Room

The War Room helps to:

- Get everyone on the same page by looking at the same real-time data
- Keep the focus on metrics that translate to the business value the application delivers
- Foster communication among a broad audience
- Identify resolution criteria and assign ownership for resolution tasks.

12.7.1.2 Widgets and Reporting

AppDynamics maintains "pre-set" functions to expedite reporting in addition to more sophisticated custom dashboard functions.

- Widgets
  - Streaming graph - updated every five seconds for a single specified node. To display streaming data from multiple nodes you need to create multiple widgets
  - Log Tail - displays the contents of the file specified by its Path
  - Issue Tracking - displays information about an issue or a list of issues that you have selected
- Scheduled Reports
  - Application Health Report
  - Dashboard Report
  - Controller Audit Report
  - Home Screen Report
  - All Applications Summary
- Pre-Configured On-Demand Reports

- Business Transaction Summary
- Business Transaction Trend
- Hardware Utilization
- Memory Utilization
- Node Performance Summary
- Node Trend

☑ *Please see https://docs.appdynamics.com/display/PRO44/Custom+Dashboards for extensive detail and videos providing instructions for custom dashboard capabilities*

12.7.2 AWS

AWS customers can leverage AWS Cloud monitoring tools such as Amazon CloudWatch, AWS Trusted Advisor, AWS Health Checks, and third-party monitoring tools to extract metrics and system analytics. The AWS Service Health Dashboard provides current and historical data across regions for each service offered. The status can be monitored in real time, or subscribed to as an RSS feed by service.

12.7.3 SERVICENOW

Administrators can view a wide range of performance metrics for their instance and for the machine on which the instance is running, displayed in a graphical format. Add these graphs and their controls to a home page to monitor the performance of instances. Some of these graphs are intended for use by ServiceNow Technical Support to troubleshoot performance issues or help tune your system for maximum efficiency. Each graph enables admins to filter the data by using different measurements, such as maximum and minimum values, means, and medians. The available graphs reflect performance in eight functional areas of ServiceNow.

- Database
- Discovery
- Disk Partitions
- Linux Stats
- Logging
- MySQL Overview
- Mode Metrics
- Replication
- ServiceNow Servlet

12.8 Printing Reports (8.12.8)

Utah Solicitation Number SK18008 Requirement: Page 29
8.12.8 Ability to print historical, statistical, and usage reports locally.

Red River has provided CSP-specific responses below.

12.8.1 AppDynamics

AppDynamics supports the ability to print historical, statistical, and usage reports locally. AppDynamics can generate and send reports as PDF files.

12.8.2 AWS

AWS provides the ability to print reports locally

12.8.3 ServiceNow

ServiceNow supports the ability to view instance performance locally. Customers can use the Customer Support Portal to obtain information about the real availability of all their instances. Real availability is the percentage of production time that an instance is up and available for use.

12.9 Support 24x365 (8.12.9)

Utah Solicitation Number SK18008 Requirement: Page 29
8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.

Red River has experience in supporting production operations with 24x7x365 deployment and configuration where we control and monitor the Managed Services Platform. Each of the CSPs maintain documentation of the standard deployment processes and areas of potential flexibility.

12.9.1 AppDynamics

☑ *Please refer to the following section for customer support expectations*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.1 AppDynamics*
- *Section 4.1 Excellent Customer Service (8.4.1) Subsection 4.1.1 AppDynamics*
- *Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018) beginning on page 141 for additional information on support expectations*

12.9.2 AWS

Auto Scaling allows customers to automatically scale their Amazon EC2 capacity up or down according to conditions that they define. Auto Scaling is well suited for applications that experience hourly, daily, or weekly variability in usage. Customers can automatically scale their Amazon EC2 fleet or maintain their Amazon EC2 fleet at a set size.

Auto Scaling enables customers to closely follow the demand curve for their applications, reducing the need to provision Amazon EC2 capacity in advance. For example, customers can set a condition to add new Amazon EC2 instances in increments of three instances to the Auto Scaling Group when the average CPU utilization of the Amazon EC2 fleet goes above 70%; and similarly, customers can set a condition to remove Amazon EC2 instances in the same increments when CPU utilization falls below 10%.

Often, customers may want more time to allow their fleet to stabilize before Auto Scaling adds or removes more Amazon EC2 instances. Customers can configure a cool down period for their Auto Scaling Group, which tells Auto Scaling to wait for some time after taking an action before it evaluates the conditions again. Auto Scaling enables customers to run their Amazon EC2 fleet at optimal utilization.

12.9.2.1 Elastic Load Balancing

Elastic Load Balancing automatically distributes incoming application traffic across multiple Amazon EC2 instances. It enables customers to achieve even greater fault tolerance in their applications, seamlessly providing the amount of load balancing capacity needed in response to incoming application traffic. Elastic Load Balancing detects unhealthy instances and automatically reroutes traffic to healthy instances until the unhealthy instances have been restored. Customers can enable Elastic Load Balancing within a single Availability Zone or across multiple zones for even more consistent application performance.

12.9.2.2 Amazon CloudWatch

Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications that customers run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, and set alarms. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon RDS database instances, as well as custom metrics generated by applications and services and any log files your applications generate. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react and keep application running smoothly.

Amazon CloudWatch's metrics and alarms can work together with Auto Scaling and ELB to dynamically deploy new instances on-demand, as depicted below.

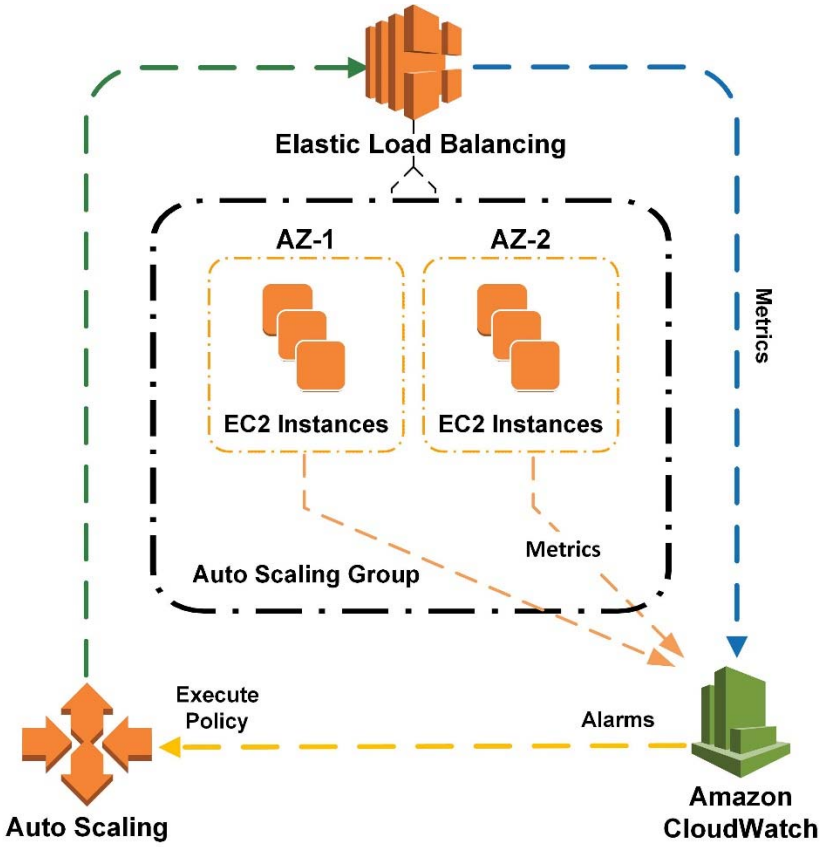


Figure 11: AWS Load Balancing

☑ *Please refer to the following section for customer support expectations*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.2 AWS*
- *Section 4.1 Excellent Customer Service (8.4.1) Subsection 4.1.2 AWS*
- *AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

12.9.3 SERVICENOW

ServiceNow provides Customer Support 24 hours a day, 7 days week, 365 days a year.

☑ *Please refer to the following section for customer support expectations*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.3 ServiceNow*
- *Section 4.1 Excellent Customer Service (8.4.1) Subsection 4.1.3 ServiceNow*
- *Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018)*

12.10 Scale-up/down (8.12.10)

Utah Solicitation Number SK18008 Requirement: Page 29
8.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

Red River has provided CSP-specific responses below.

12.10.1 APPDYNAMICS

AppDynamics will automatically scale the platform based upon need. It will do this in both a horizontal and vertical model dependent upon the load of the platform. It will be scaled by the AppDynamics team. The platform will be available on a full 24x365 basis.

☑ *Please refer to the following section for scale up/scale down expectations*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.1 AppDynamics*
- *Section 4.1 Excellent Customer Service (8.4.1) Subsection 4.1.1 AppDynamics*
- *Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018)*

12.10.2 AWS

☑ *Please see our response in Section 12.9 Support 24x365 (8.12.9) Subsection 12.9.2 AWS*

12.10.3 SERVICENOW

ServiceNow can automatically scale its application servers horizontally by adding or subtracting them to the load balancer pools for a particular instance. Scaling is managed by the ServiceNow Cloud Operations team.

☑ *Please refer to the following section for customer support expectations*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.3 ServiceNow*
- *Section 4.1 Excellent Customer Service (8.4.1) Subsection 4.1.3 ServiceNow*
- *Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018)*

13. (E) CLOUD SECURITY ALLIANCE (8.13)

13.1 CSA Star Registry (8.13.1)

Utah Solicitation Number SK18008 Requirement: Page 29
Describe and provide your level of disclosure with CSA Star Registry for each Solution offered.
a. Completion of a CSA STAR Self-Assessment. (3 points)
b. Completion of Exhibits 1 and 2 to Attachment B. (3 points)
c. Completion of a CSA STAR Attestation, Certification, or Assessment. (4 points)
d. Completion CSA STAR Continuous Monitoring. (5 points)

Red River has described and provided our level of disclosure with CSA Star Registry for each Solution offered.

13.1.1 APPDYNAMICS

AppDynamics provides the following:

- **CSA STAR Level 1: CSA STAR Self-Assessment** - AppDynamics has completed the CSA STAR Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B
- **CSA STAR Level 2: CSA STAR Attestation and Certification -** Per the CSA definitions, AppDynamics aligns with the CSA STAR Attestation and Certification via the determinations in our third-party audits for SOC and ISO. CSA STAR Level 2 Attestation is based on SOC2, which can be provided under NDA
- **CSA STAR Level 3: Continuous Monitoring -** As noted on the CSA website, Level 3 Continuous Monitoring requirements are in development. ServiceNow cannot define alignment, but does provide clients with extensive continuous monitoring tools for full transparency

13.1.2 AWS

AWS provides the following:

- **CSA STAR Level 1: CSA STAR Self-Assessment** - AWS has completed the CSA STAR Self-Assessment and published the results to the AWS website. Please refer to the CSA Consensus Assessments Initiative Questionnaire. This is the latest CAIQ (v3) released by the CSA.
- **CSA STAR Level 2: CSA STAR Attestation and Certification -** Per the CSA definitions, AWS aligns with the CSA STAR Attestation and Certification via the determinations in our third-party audits for SOC and ISO. CSA STAR Level 2 Attestation is based on SOC2, which can be requested with AWS Artifact - The SOC 2 report audit attests that AWS has been validated by a third-party auditor to confirm that AWS' control objectives are appropriately designed and operating effectively. CSA STAR Level 2 Certification is based on ISO 27001:2005.

- **CSA STAR Level 3: Continuous Monitoring -** As noted on the CSA website, CSA is still defining the Level 3 Continuous Monitoring requirements. Although, for this reason, AWS cannot determine alignment, AWS does provide customers with the tools they need to meet continuous monitoring requirements. Customers can leverage the AWS Security by Design (SbD) program by providing control responsibilities outlines, the automation of security baselines, the configuration of security and the customer audit of controls for AWS customer infrastructure, operating systems, services and applications running in AWS. This standardized, automated, prescriptive and repeatable design can be deployed for common use cases, security standards and audit requirements across multiple industries and workloads. For more information visit the Security by Design page.

13.1.3 SERVICENOW

ServiceNow provides the following:

- **CSA STAR Level 1: CSA STAR Self-Assessment** - ServiceNow has completed the CSA STAR Self-Assessment and can be downloaded from the CSA site https://cloudsecurityalliance.org/registry/servicenow /
- **CSA STAR Level 2: CSA STAR Attestation and Certification -** ServiceNow aligns with the CSA STAR Attestation and Certification via the determinations in our third-party audits for SOC and ISO. CSA STAR Level 2 Attestation is based on SOC2, which is provided to potential clients under NDA
- **CSA STAR Level 3: Continuous Monitoring -** As noted on the CSA website, Level 3 Continuous Monitoring requirements are in development. ServiceNow cannot define alignment, but does provide clients with extensive continuous monitoring tools for full transparency.

14. (E) SERVICE PROVISIONING (8.14)

14.1 Emergency or Rush Services (8.14.1)

Utah Solicitation Number SK18008 Requirement: Page 29
8.14. 1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

Red River has experience in supporting production operations with 24x7x365 deployment and configuration where we control and monitor the Managed Services Platform. Each of the CSPs maintain documentation of the standard deployment processes and areas of potential flexibility.

14.1.1 APPDYNAMICS

AppDynamics orchestrates our services needs on a first come first-serve basis. Once a contract is executed to understand the services to be delivered, we will then schedule the resources for delivery. AppDynamics maintains provisions for certain rush services or services outside normal business hours that can be established for clients.

14.1.2 AWS

AWS uses the term “elastic” to describe the ability to scale computing resources up and down easily, with minimal friction. Elasticity helps you avoid provisioning resources up front for projects with variable consumption rates or short lifetimes. Instead of acquiring hardware, setting it up, and maintaining it in order to allocate resources to your applications, you use AWS to allocate resources using simple Application Program Interface (API) calls. Elastic Load Balancing and Auto Scaling can automatically scale your AWS cloud-based resources up to meet unexpected demand, and then scale those resources down as demand decreases.

14.1.3 SERVICENOW

ServiceNow professional services organization responds to customer needs based on each request. Once a purchase order is received from the Purchasing Entity, ServiceNow contacts the Customer to discuss schedules. Resources are assigned based on the project need. If the customer has a priority issue with the system, they would open a ticket and the ticket SLA process would proceed until the issue is resolved. Every ServiceNow customer is supported based on their priority and need.

14.2 Lead-Time for Provisioning (8.14.2)

Utah Solicitation Number SK18008 Requirement: Page 29
8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

Red River has provided CSP-specific responses below.

14.2.1 APPDYNAMICS

AppDynamics has an automated back end system for provisioning the cloud environment for SaaS based deployments. There is a manual process for converting an executed contract to our automated system. Within two business days is the standard lead time for such processes

14.2.2 AWS

☑ *Please see our response in Section 14.1 Emergency or Rush Services (8.14.1) Subsection 14.1.2 AWS*

14.2.3 SERVICENOW

ServiceNow provisions new instances or newly purchased users or applications to the instance within 48 hours after receipt of order. If users or applications are required more quickly, the customer controls access to all ServiceNow capabilities at any time and the true-up occurs thereafter.

15. (E) BACK UP AND DISASTER PLAN (8.15)

15.1 Retention Periods (8.15.1)

Utah Solicitation Number SK18008 Requirement: Page 29
8.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

Red River has provided CSP-specific responses below.

15.1.1 AppDynamics

AppDynamics maintains metrics in one-minute increments (retained for 4 hours), ten-minute increments (retained for 48 hours) and one-hour increments (retained for 365 days).

☑ *Please refer to https://docs.appdynamics.com/display/PRO44/License+Entitlements+and+Restrictions for greater detail on data retention provisions*

15.1.2 AWS

AWS customers control the entire life-cycle of their content on AWS, and manage their content in accordance with their own specific needs, including content classification, access control, retention and deletion.

15.1.3 ServiceNow

Once notified ServiceNow has the ability to leverage our internal clone operation process. This provides a locked state copy of the instance, while the customer can continue working on the production instance. Any data additions, changes or deletes will be on the production but not on the frozen instance copy. Additionally, ServiceNow can freeze backups to prevent them from being over written.

15.2 Risks and Mitigations (8.15.2)

Utah Solicitation Number SK18008 Requirement: Page 29
8.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

Red River has worked collaboratively with clients to identify and define disaster recovery provisions. At the highest level, our client engagements emphasize that backup is not disaster recovery and that disaster recovery is not just a CSP responsibility - it involves:

- People – Red River and NASPO/ValuePoint understand the importance of a single point of contact for contract and compliance of the underlying MSA as well as a point of

contact to exercise incident management. Points of Contact are more important when a Sev1 or Priority 1 rises to the potential declaration of a disaster. The "people" element incorporates alignment of the client business organization that use the services and the client IT organization that supports the local infrastructure. All stakeholder communities need to be identified so a critical link is not discovered during a disaster

- Functions and Components – the industry has generally reflected that "cloud" provides scalability and redundancy that is more challenging to structure in an on-premise environment. At the same time, there are elements that still may still reflect "on-premise" by their nature – network infrastructure outside the CSP (e.g., dedicated circuits to physical locations), local compute capacities that help manage services, or facilities themselves and their related wiring (or wireless), cooling and similar elements that impact the end-to-end use of the CSP-provided service.
- Processes – The "people" must be clearly defined in their relationship to a documented process – the stakeholders, facilities, internal populations, external populations and other groups must be specifically referenced with roles and responsibilities.

Under all engagements, we emphasize the importance of the collaborative development – and practice exercise – of a comprehensive Disaster Recovery Plan that addresses the continuum of possible risks and mitigations. Our approach to client engagements follows a framework:

- Business Impact Analysis (BIA) - a comprehensive backup and DR planning process must begin with an assessment of your AS IS and TO BE virtualized environment, such as data size, location, and criticality. Resumption requirements must be tied to tangible loss and intangible loss for Red River and the client to right-size the DR infrastructure to the extent of loss.
- Risk Assessment – translate your BIA to the threat of external events and the external mitigation activities (e.g., prior disruptive events, weather, vendor history)
- Mitigation – Red River has worked in different client engagements with a wide variety of potential disaster dynamics (e.g., Brown-out in California's Enron days, earthquakes, DoD). The only "best practice" is a collaborative evaluation of each risk for the options to mitigate, or the hierarchy of mitigation – the collaboration is the key piece of mitigation.
- Document, Train, and Practice Test – Red River Managed Services exercises DR procedures on at least a semi-annual basis – full scale drop and recovery in virtualized services. Red River resources, as highlighted by Section 17 (E) INTEGRATION AND CUSTOMIZATION (8.18) on page 114 and Section 19 (E) RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS (8.20) on page 128, can augment base CSP DR activities up to and including customized provisions around the CSP offering and integrated with client operations.

15.2.1 APPDYNAMICS

AppDynamics has designed its SaaS architecture with fault tolerance in mind and leverages the multi-availability zone and multi-region capabilities of Amazon Web Services. By policy, AppDynamics does not provide details on internal risk assessments to customers but can provide summaries to clients under NDA.

15.2.2 AWS

Our infrastructure has a high level of availability and we provide you with the features you need to deploy a resilient IT architecture. Our systems are designed to tolerate system or hardware failures with minimal customer impact. The AWS Cloud supports many popular disaster recovery architectures, ranging from “pilot light” environments that are ready to scale up at a moment’s notice to “hot standby” environments that enable rapid failover. All data centers are online and serving customers; no data center is “cold.” In the case of a failure, automated processes move your data traffic away from the affected area. By distributing applications across multiple AWS Availability Zones, you can remain resilient in the face of most failure modes, including natural disasters or system failures. You can build highly resilient systems in the cloud by employing multiple instances in multiple AWS Availability Zones and using data replication to achieve extremely high recovery time and recovery point objectives. You are responsible for managing and testing the backup and recovery of your information system that is built on the AWS infrastructure. You can use the AWS infrastructure to enable faster disaster recovery of your critical IT systems without incurring the infrastructure expense of a second physical site.

☑ *Please see https://aws.amazon.com/disaster-recovery/ for extensive detail on DR provisions*

15.2.3 SERVICENOW

ServiceNow is divided into two distinct environments for Business Continuity (BC) and Disaster Recovery (DR). ServiceNow’s corporate environment and its data center environments are physically and logically isolated from each other. A disaster in ServiceNow’s corporate environment could occur with little or no impact on the ability for the data centers within the private cloud to operate. In both cases, the BC and the DR are supported by a series of Standard Operating Procedures (SOPs) that allow ServiceNow to quickly and effectively take action when it is required.

ServiceNow's customer DR is documented in an Information System Contingency Plan, which covers its data center environments, and includes all customer environments as well as the instances that ServiceNow uses to run its business. ServiceNow formally tests this process on an annual basis and can produce compliance reports for customers requiring them. ServiceNow also uses the process of transferring instances to reduce the impact of maintenance on its service and will move instances out of one data center to the other on a daily basis. As a result, ServiceNow is very practiced at the process of "failing over" customer instances.

15.3 Data Center Infrastructure (8.15.3)

Utah Solicitation Number SK18008 Requirement: Page 29
8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

Red River has provided CSP-specific responses below.

15.3.1 AppDynamics

AppDynamics has designed its SaaS architecture with fault tolerance in mind and leverages the multi-availability zone and multi-region capabilities of Amazon Web Services.

15.3.2 AWS

The AWS Cloud infrastructure is built around regions and Availability Zones. A region is a physical location in the world where we have multiple Availability Zones. Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity and housed in separate facilities. These Availability Zones offer customers the ability to operate production applications and databases that are more highly available, fault tolerant, and scalable than would be possible with a single data center.

AWS currently has 18 regions, 54 Availability Zones, and 1 Local Region throughout the world: US East (Northern Virginia), US East (Ohio), US West (Oregon), US West (Northern California), AWS GovCloud (US-West), Canada (Central), EU (Ireland), EU (Frankfurt), EU (London), EU (Paris), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), Asia Pacific (Seoul), Asia Pacific (Mumbai), Asia Pacific (Osaka-Local), South America (Sao Paulo), China (Beijing), and China (Ningxia). Information on each region can be found at the AWS Global Infrastructure webpage. Figure 12: AWS Availability Zones depicts the current AWS Regions and Availability Zones, along with the four new regions that AWS has announced plans for. The AWS products and services that are available in each region are listed at the Region Table webpage.

Figure 12: AWS Availability Zones

Figure 13: Availability Zone illustrates the relationship between regions and Availability Zones.

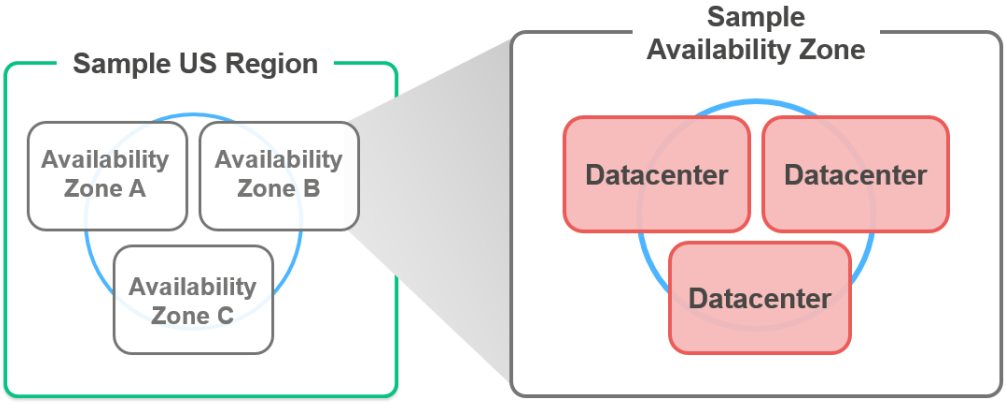


Figure 13: Availability Zone

15.3.3 SERVICENOW

ServiceNow's data centers and cloud-based infrastructure have been designed to be highly available. All servers and network devices have redundant components and multiple network paths to avoid single points of failure. At the heart of this architecture, each customer application instance is supported by a multi-homed network configuration with multiple connections to the Internet. Production application servers are load balanced within each data center. Production database servers are replicated in near-real time to a peer data center within the same geographic region. ServiceNow leverages this Advanced High Availability (AHA) architecture for customer production instances in several ways:

- In the event of the failure of one or more infrastructure components, service is restored by transferring the operation of customer instances associated with the failed components to the peer data center.
- Before executing required maintenance, ServiceNow can proactively transfer operation of customer instances impacted by the maintenance to the peer data center. The maintenance can then proceed without impacting service availability.

This approach means that the transfer between active and standby data centers is being regularly executed as part of standard operating procedures – ensuring that when it is needed to address a failure, the transfer will be successful and service disruption minimized.

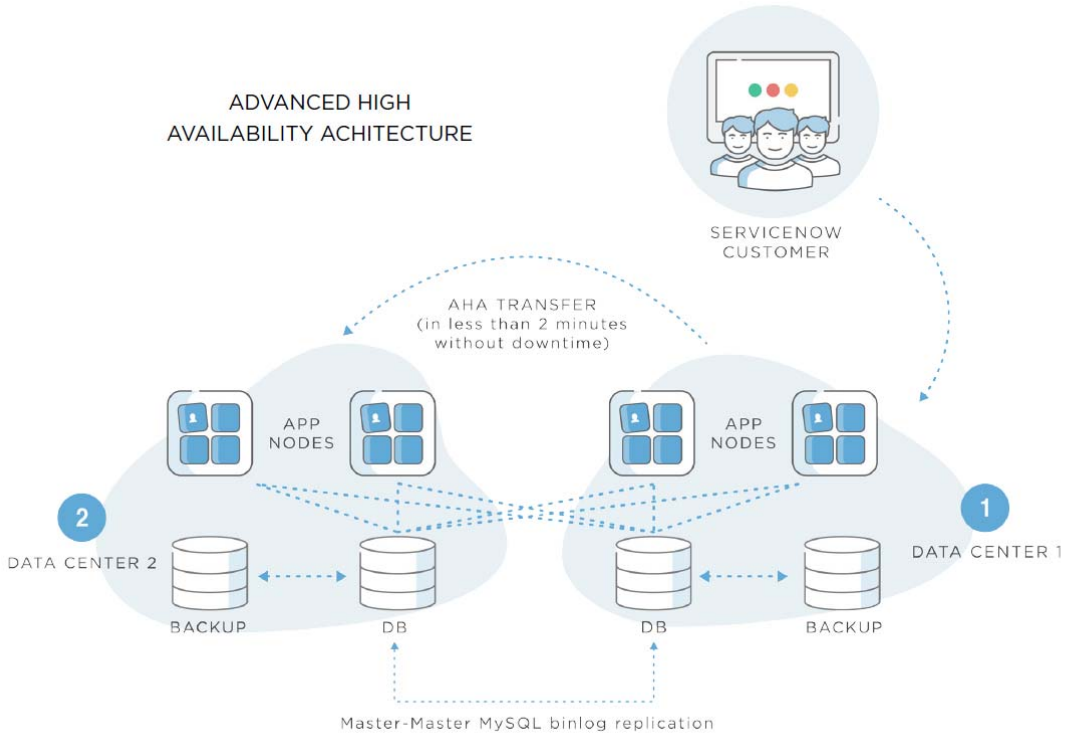


Figure 14: High Availability Diagram

15.4 Documentation (8.16.1)

Utah Solicitation Number SK18008 Requirement: Page 29 *8.16.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.*

Red River maintains an extensive set of documentation for both our corporate operations and for specific client engagements – we enjoy nimble and we treasure documentation to establish clarity of expectations and activities. Each CSP provides documentation, as described below, for their unique operations.

15.4.1 APPDYNAMICS

AppDynamics maintains extensive documentation in their support portal (https://docs.appdynamics.com/), including specific drill-downs for provisioning processes (https://docs.appdynamics.com/display/PRO44/AppDynamics+Platform). The nature of AppDynamics provisioning is closely associated with the target environment – specifically when and where to deploy the agents and how to connect back to the controller. AppDynamics provides a Deployment Roadmap to guide administrators with the steps to "go live."

15.4.2 AWS

The AWS Management Console is a single destination for managing all AWS resources, from Amazon Elastic Compute Cloud (Amazon EC2) instances to Amazon DynamoDB tables. Customers can use the AWS Management Console to perform any number of tasks, from deploying new applications to monitoring the health of applications. The AWS Management Console also enables customers to manage all aspects of their AWS account, including accessing monthly spending by service, managing security credentials, or even setting up new AWS Identity and Access Management (AWS IAM) users. The AWS Management Console supports all AWS Regions and lets customers provision resources across multiple regions.

The AWS Command Line Interface (CLI) is a unified tool used to manage AWS Cloud services. With just one tool to download and configure, customers can control multiple AWS resources from the command line and automate them through scripts. The AWS CLI introduces a new set of simple file commands for efficient file transfers to and from Amazon Simple Storage Service (Amazon S3).

15.4.3 SERVICENOW

ServiceNow provides a library of documentation for its SaaS offering (https://docs.servicenow.com/) as well as extensive detail for provisioning (https://docs.servicenow.com/category/kingston) that highlights steps for the primary administrator, including

- Core configuration
- Table administration
- List administration
- Form configuration
- Form administration
- Field administration
- State Management.

- Currency administration
- Localization settings
- Localization settings control translation, currency, and locale settings in the instance.
- Time configuration
- Search administration
- Events
- Data management
- Integration with third-party applications and data sources
- User administration
- Platform performance
- Upgrades and conversions
- System security

15.5 Tool Sets (8.16.2)

Utah Solicitation Number SK18008 Requirement: Page 29
8.16.2 Provide tool sets at minimum for:

1. *Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)*
2. *Creating and storing server images for future multiple deployments*
3. *Securing additional storage space*
4. *Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).*

Red River has provided CSP-specific responses below.

15.5.1 AppDynamics

AppDynamics has read and understands this requirement. The AppDynamics offering in this proposal is SaaS, with on-premise offerings targeting server images, space and other provisions also available. AppDynamics operates under Cisco Systems, Inc.'s master agreement with AWS.

AppDynamics provides toolsets unique to a roster of targeted applications, extensions and monitoring:

- Application languages - Java, .NET, PHP, C++, Node.js, Python, GO,
- Cloud and Infrastructure – MS Azure, Citrix, CloudWeaver, Docker, Ehcache, Elastisearch, Google, HP, Joyent, Logstash, BMV BPPM, OpenShift, OpenStack, Oracle, Pivotal Cloud Foundry, Rackspace, Splunk, VMWare vCloud and vSphere, Oracle Weblogic, Websphere, Kubernetes, AWS

- DevOps – Jenkins, OpsGenie, VictorOps
- Server – AMPS, Apache, F5, HA Proxy, TibcoEMS, Tomcat, vSphere
- Databases – Amazon, DB2, MongoDB, MySQL, Oracle, PostgreSQL, SQL Server, Sybase, VoltDB
- Incident Management Systems – ServiceNow, PagerDuty, Jira
- Mobile – iOS, Android, IoT

15.5.2 AWS

AWS offerings are provided with a range of supporting components like management tools, networking services, and application augmentation services, with multiple interfaces to AWS Application Programming Interface (API)-based services, including Software Development Kits (SDKs), Integrated Development Environment (IDE) toolkits, and Command Line Tools: http://aws.amazon.com/tools/.

Tool	Description
Developer Tools	The AWS Developer Tools help you securely store and version control your application's source code and automatically build, test, and deploy your application to AWS or your on-premises environment. • AWS CodeCommit is a fully-managed source control service that makes it easy for companies to host secure and highly scalable private Git repositories. AWS CodeCommit eliminates the need to operate a source control system or worry about scaling its infrastructure. Customers can use AWS CodeCommit to securely store anything from source code to binaries, and it works seamlessly with existing Git tools. • AWS CodePipeline is a continuous integration and continuous delivery service for fast and reliable application and infrastructure updates. AWS CodePipeline builds, tests, and deploys a customer's code every time there is a code change, based on the release process models they define. This enables customers to rapidly and reliably deliver features and updates. Customers can easily build out an end-to-end solution by using our pre-built plugins for popular third-party services like GitHub or integrating custom plugins into any stage of the release process. With AWS CodePipeline, customers only pay for what they use. There are no upfront fees or long-term commitments. • AWS CodeBuild is a fully managed build service that compiles source code, runs tests, and produces software packages that are ready to deploy. With AWS CodeBuild, customers don't need to provision, manage, and scale their own build servers. AWS CodeBuild scales continuously and processes multiple builds concurrently, so builds are not left waiting in a queue. Customers can get started quickly by using prepackaged build environments, or they can create custom build environments that use their own build tools. With AWS CodeBuild, customers are charged by the minute for the compute resources they use.

Tool	Description
	• AWS CodeDeploy is a service that automates code deployments to any instance, including Amazon EC2 instances and instances running on-premises. AWS CodeDeploy makes it easier for customers to rapidly release new features, helps them avoid downtime during application deployment, and handles the complexity of updating their applications. Customers can use AWS CodeDeploy to automate software deployments, eliminating the need for error-prone manual operations. The service also scales with infrastructure so customers can easily deploy to one instance or thousands. • Language/platform-specific SDKs: Java, .NET, Node.js, PHP, Python, Ruby, Browser, Go, C++ • AWS IoT Device SDK • AWS Mobile SDKs: Android, iOS, React Native, Mobile Web, AWS Mobile SDK • IDE Mobile SDKs: Eclipse, Visual Studio, VSTS • Serverless Development Tools • AWS Serverless Application Model (AWS SAM) is a model to define serverless applications. AWS SAM is natively supported by AWS CloudFormation and provides a simplified way of defining the Amazon API Gateway APIs, AWS Lambda functions, and Amazon DynamoDB tables needed by your serverless application. The specification is available under Apache 2.0. Learn more in our documentation. • AWS SAM Local is a CLI tool that allows you to locally test and debug your AWS Lambda functions defined by AWS Serverless Application Model (SAM) templates. SAM Local can be used to test functions locally, start a local API Gateway from a SAM template, validate a SAM template, and generate sample payloads for various event sources.
Resource Provisioning	• AWS CloudFormation gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. Customers can use AWS CloudFormation's sample templates or create their own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run their application. • AWS Marketplace is an online store that helps customers find, buy, and immediately start using the software and services they need to build products and run their businesses. AWS Marketplace features many software categories including databases, application servers, testing tools, monitoring tools, content management, and business intelligence. Visitors to AWS Marketplace can use 1-Click deployment to quickly launch pre-configured software and pay only for what they use, by the hour or month. AWS handles billing and payments, and software charges appear on customers' AWS bill. • AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows

Tool	Description
	customers to centrally manage commonly deployed IT services, helps them achieve consistent governance, and helps them meet their compliance requirements, all while enabling users to quickly deploy only the approved IT services they need.
Configuration Management	• AWS OpsWorks is a configuration management service that helps customers configure and operate applications of all shapes and sizes using Chef. Customers can define the application's architecture and the specification of each component including package installation, software configuration, and resources such as storage. Customers can start from templates for common technologies like application servers and databases or build their own to perform any task that can be scripted. AWS OpsWorks includes automation to scale applications based on time or load and dynamic configuration to orchestrate changes as an environment scales. • AWS Systems Manager allows customers to centralize operational data from multiple AWS services and automate tasks across AWS resources. Customers can create logical groups of resources such as applications, different layers of an application stack, or production versus development environments. With AWS Systems Manager, customers can select a resource group and view its recent API activity, resource configuration changes, related notifications, operational alerts, software inventory, and patch compliance status. AWS Systems Manager provides a central place to view and manage AWS resources, so customers can have complete visibility and control over their operations.
Monitoring and Performance	• Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications that customers run on AWS. Customers can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in their AWS resources. Amazon CloudWatch can monitor AWS resources such as Amazon EC2 instances, Amazon DynamoDB tables, and Amazon Relational Database Service (Amazon RDS) DB instances, as well as custom metrics generated by the customer's applications and services and any log files their applications generate. Customers can use Amazon CloudWatch to gain system-wide visibility into resource utilization, application performance, and operational health and then use those insights to react and keep their application running smoothly.
Governance and Compliance	• AWS Config is a fully managed service that provides customers with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. AWS Config Rules enables customers to create rules that automatically check the configuration of AWS resources recorded by AWS Config. With AWS Config, customers can discover existing and deleted AWS resources, determine their overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting. • AWS CloudTrail is a web service that records AWS API calls for a customer's account and delivers log files to them. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the

Tool	Description
	API caller, the request parameters, and the response elements returned by the AWS Cloud service. With AWS CloudTrail, customers can get a history of AWS API calls for their account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS Cloud services (such as AWS CloudFormation). The AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing. • AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows customers to centrally manage commonly deployed IT services, helps them achieve consistent governance, and helps them meet their compliance requirements, all while enabling users to quickly deploy only the approved IT services they need.
Resource Optimization	• AWS Trusted Advisor is an online resource to help customers reduce cost, increase performance, and improve security by optimizing their AWS environment. AWS Trusted Advisor provides real-time guidance to help customers provision their resources following AWS best practices.

Table 13: AWS Tools

15.5.3 SERVICENOW

ServiceNow has read and understands this requirement. ServiceNow supports only a SaaS environment so there is no on-premise offering.

16. (E) TRIAL AND TESTING PERIODS (PRE- AND POST- PURCHASE) (8.17)

16.1 Testing and Training Periods (8.17.1)

Utah Solicitation Number SK18008 Requirement: Page 29
8.17.1 Describe your testing and training periods that your offer for your service offerings.

Training and testing periods will vary based on the CSP as well as the complexity of the request that is made by the Purchasing Entity. Some of the services can be functional within a few days and some will take a few months for full implementation. Red River will work collaboratively with potential clients and the CSP to define specific test and training periods. Red River has provided CSP-specific responses below.

16.1.1 AppDynamics

AppDynamics is a solution tailored for immediate return on your investment. Out of the box, with little configuration, the platform is learning your "normal" application and infrastructure behavior. Certain features of the solution require additional business insight and configuration.

16.1.2 AWS

The AWS Free Tier is designed to enable potential customers to get hands-on experience with over 25 AWS Cloud Services. The AWS Free Tier includes services with a free tier available for 12 months following the AWS sign-up date, as well as additional service offers that do not automatically expire at the end of the 12-month AWS Free Tier term. AWS's free usage tier is not limited to specific use cases

16.1.3 ServiceNow

ServiceNow strives to get customers up and running quickly as it is a SaaS application. Training and testing periods will vary based on the complexity of the request that is made by the Purchasing Entity.

16.2 Testing and Training Periods (8.17.2)

Utah Solicitation Number SK18008 Requirement: Page 29
8.17.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

Red River has provided CSP-specific responses below.

16.2.1 APPDYNAMICS

AppDynamics will conduct a proof of concept in an environment (where application load is present) of your choice. We will provide a survey understanding your environment and business objective. We will showcase how to identify performance bottlenecks, root cause scenarios, end user monitoring, and showcasing our Business IQ platform.

16.2.2 AWS

☑ *Please see our response in Section 16.1Testing and Training Periods (8.17.1) Subsection 16.1.2 AWS*

16.2.3 SERVICENOW-VALIDATE SN

ServiceNow will provide access to our technology which may be in a limited or "DEMO" fashion. Access will be to an extent that the State may complete any necessary tests or verifications that may be required. Instructions on precisely how each technology will be accessed will be provided upon request. A specific instance of the requested technology would be stood up within the cloud framework to support this request.

16.3 Training and Support (8.17.3)

Utah Solicitation Number SK18008 Requirement: Page 30
8.17.3 Offeror must describe what training and support it provides at no additional cost.

The 3 CSPs proposed by Red River all offer extensive networks of free training and support. We will work collaboratively with potential clients to help map the network of free information to their specific implementation needs. Red River has provided CSP-specific responses below.

16.3.1 APPDYNAMICS

AppDynamics offers fully documented support via an easy to use web portal. Included with the software procurement is standard support offering troubleshooting of the AppDynamics platform. You can also visit our University Portal for self-paced learning material included with your subscription at no additional cost.

16.3.2 AWS

AWS provides a mature infrastructure for training and support – from ad hoc/wiki-style through structured learning paths.

☑ *Please refer to https://aws.amazon.com/training/ for an extensive outline of the latest free offerings in the AWS catalog*

16.3.3 SERVICENOW

ServiceNow is actively working on a process to allow eligible customers advance access to upcoming product Family Releases so they may review what features and functionality will be available in the next forthcoming release. New Family Releases are made generally available approximately every six (6) months but may be longer or shorter depending upon functionality enhancements. ServiceNow provides an extensive library of free training and support from Q&A through training and certification paths.

☑ *Please refer to https://www.servicenow.com/services/training-and-certification.html for an extensive outline of the latest free offerings in the ServiceNow catalog*

17. (E) INTEGRATION AND CUSTOMIZATION (8.18)

17.1 Integration (8.18.1)

Utah Solicitation Number SK18008 Requirement: Page 30
8.18.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

Red River maintains an Enterprise Application Division (EAD) that specializes in the spectrum of integration across applications and infrastructure – from custom-developed solutions to integration using industry conventions (e.g., REST APIs, CLI, and shell scripting) to exercising native connectors in Commercial-off-the-Shelf tools to enabling infrastructure integration around multiple CSPs, Hybrid Cloud and other multi-platform implementation.

Our proposed CSPs provide access servers, storage, databases, and a broad set of application services via a web application, mobile client, or programmatically through published and well documented APIs. These API's allow programmers an opportunity to develop applications that are more scalable, flexible and infrastructure aware. While integration into other applications vary with each cloud service provider, it is standard practice to allow for open APIs for integration development. For Example, AWS IaaS and PaaS services are fully documented and ready to integrate into third party applications via REST APIs, CLI, and shell scripting.

17.1.1 AppDynamics

The AppDynamics Application Intelligence Platform integrates with Platform as a Service (PaaS) providers, providing easily implemented AppDynamics monitoring for cloud or PaaS-hosted applications. In general, the integration allows developers to add AppDynamics app agent instrumentation to their applications as additional service when provisioning their application host instance. In some cases, AppDynamics can provide machine-level monitoring information for the virtual platform and supporting infrastructure.

17.1.1.1 PaaS Provider Integration

The following section lists the PaaS providers with which the AppDynamics platform integrates. For details on how to use the AppDynamics specific platforms, see the documentation listed.

- Pivotal Cloud Foundry (PCF) Application and machine monitoring in PCF environments. AppDynamics can provide built in support for these Cloud Foundry buildpacks:
    - Java Buildpack 3.4 and higher. (See Using AppDynamics with Java Applications on Pivotal Cloud for a walkthrough of using the Java Buildpack.)
    - PHP Buildpack 4.0+. (See Using AppDynamics with PHP Applications on Pivotal Cloud Foundry for a walkthrough of using the PHP Buildpack.)
    - For more and updated information and a link to the AppDynamics tile page, see the AppDynamics APM Tile documentation.

- Red Hat OpenShift 3 Docker images with built-in AppDynamics monitoring support for JBoss EAP 6.4 and WildFly 8.1. For documentation and download information, see the AppDynamics Java APM Agent page on the Red Hat Customer Portal.
- Microsoft Azure - You can use NuGet or the Windows Azure Portal to install the AppDynamics .NET Agent package directly to projects you run in Windows Azure. You can instrument Web Roles, Worker Roles, and App Services. For more information, see Deploy AppDynamics for Azure.

17.1.1.2 Extensions and APIs

The AppDynamics Community Exchange includes many extensions that supplement the capabilities of the AppDynamics App iQ Platform. Documentation on setting up and using the integration module appears with the module. Table 14: AppDynamics Integration Modules highlights modules built into the AppDynamics platform.

Integration Module	More information
Apica	Apica & AppDynamics
Atlassian JIRA	Integrate AppDynamics with Atlassian JIRA
DB CAM	Integrate AppDynamics with DB CAM
Scalyr	Integrate AppDynamics with Scalyr
Splunk	Integrate AppDynamics with Splunk
Compuware Strobe	Integrate AppDynamics with Compuware Strobe
AppDynamics for Databases	Integrate AppDynamics for Databases with AppDynamics Pro 3.7 and higher

Table 14: AppDynamics Integration Modules

Alternatively, you can use the AppDynamics REST APIs to create custom integrations and custom automation tasks. The AppDynamics Application Intelligence Platform exposes various APIs for customizing and extending its features. Generally speaking, they can be categorized as platform-side APIs, which are served by the Controller and Events Service, and agent-side APIs.

The AppDynamics platform server components and agents offer the following APIs:

- Controller APIs: Use to administer the Controller, configure, monitor, query metrics, and more. For documentation see the Platform API Index, below.
- Analytics Events API: Use to send custom analytics events from your own data sources to the Events Service. For documentation see the Analytics Events API section in the Platform API Index, below.
- Standalone Machine Agent APIs: HTTP APIs available at the machine agent for uploading custom metrics. See Standalone Machine Agent HTTP Listener.
- Database Agent APIs: Use to get, create, update, and delete Database Monitoring database Collectors

- Application Agent Instrumentation APIs: Use to control and customize transaction detection and correlation, along with exit point detection. The agent APIs include:
  - PHP Agent API
  - Python Agent API
  - Node.js Agent API Reference
  - C/C++ Application Agent
  - Java Agent API: Customize agent instrumentation. See the SDK folder in the agent home directory
- Mobile RUM: Instrument mobile applications for real user performance monitoring. See Instrument iOS Applications for more information.
- Cloud Connector API: Use to integrate cloud auto-scaling features with new platforms. See Custom Cloud Connectors.

Table 15: AppDynamics API Roster highlights methods in the AppDynamics Controller and Events Service APIs:

Controller and Event APIs	Description
Accounts	This API is documented using Swagger-based REST browser. For more information, see Using the Controller APIs.
Application Model	• Retrieve All Business Applications • Retrieve All Business Transactions in a Business Application • Retrieve All Tiers in a Business Application • Retrieve All Registered Backends in a Business Application with Their Properties • Retrieve Node Information for All Nodes in a Business Application • Retrieve Node Information by Node Name • Retrieve Node Information for All Nodes in a Tier • Retrieve Tier Information by Tier Name
Metric and Snapshot	• Retrieve Metric Hierarchy • Retrieve Metric Data • Retrieve Transaction Snapshots • Retrieve Controller Audit History • Configure Metric Retention by Account • Configure Metric Retention by Application
Alert and Respond	• Retrieve All Health Rule Violations in a Business Application

Controller and Event APIs	Description
	• Retrieve Event Data • Create Events • Create a Custom Event • Create Custom URLS for Notifications • Create and Delete Action Suppressions • Retrieve All Existing Action Suppressions • Retrieve a Specific Action Suppression by ID • Create a New Action Suppression • Delete a Specific Action Suppression by ID
Configuration	• Create and Modify AppDynamics Users • Include or exclude a business transaction from monitoring • Retrieve All Controller Settings • Retrieve a Controller Setting by Name • Configure Global Controller Settings • Mark Nodes as Historical
Configuration Export and Import	• About the Configuration Import/Export APIs • Export Actions from an Application • Import Actions into an Application • Export Email Action Templates from an Account • Import Email Action Templates • Export HTTP Request Action Templates from an Account • Import HTTP Action Templates into an Account • Export Custom Dashboards and Templates • Import Custom Dashboards and Templates • Export Health Rules from an Application • Import Health Rules into an Application • Export Transaction Detection Rules for All Entry Point Types • Import Transaction Detection Rules for All Entry Point Types • Export a Transaction Detection Rule for an Entry Point Type • Import Transaction Detection Rule for an Entry Point Type
Analytics Events	• About the Analytics Events API • Publish Events • Create Event Schema • Retrieve Event Schema • Update Event Schema

Controller and Event APIs	Description
	• Delete Event Schema • Query Events (Single Query) • Query Events (Multiple Queries)
RBAC	• Create User • Get User by ID • Get User by Name • Get All Users • Update User • Delete User • Create Group • Get Group by ID • Get Group by Name • Get All Groups • Update Group • Delete Group • Add User to Group • Remove User from Group • Create Role • Add Role to User • Remove Role from User • Add Role to Group • Remove Role from Group • Get Role by ID • Get Role by Name • Get All Roles • Update Role • Delete Role

Table 15: AppDynamics API Roster

17.1.2 AWS

AWS maintains an extensive Marketplace of integration and customization tools. The roster below is a highlight of key integration enablers

- Amazon Virtual Private Cloud (Amazon VPC). Within a logically isolated network, Amazon VPC provides complete control over the virtual networking environment,

including selection of IP address ranges, creation of subnets, and configuration of route tables and network gateways.

- Amazon Direct Connect. AWS Direct Connect can establish a dedicated network connection between AWS and a customer's datacenter, office, or colocation environment.
- Data Integration and Lifecycle Management. Once the customer's architecture is connected to the cloud, AWS can ensure this data is reliably backed-up, help control where data is placed, replicate data across geographic regions, manage the lifecycle of data, or even have datacenter topology close enough to enable synchronous replication.
- AWS Storage Gateway. Available for download as a virtual machine (VM), customers install it on a host in the datacenter and use the AWS Management Console to create either Gateway-Cached or Gateway-Stored storage volumes that can be mounted as iSCSI devices by the on-premises applications.
- Amazon Simple Storage Service. A highly durable, scalable, and secure storage infrastructure that is well suited for backing up and archiving critical data.
- Amazon Glacier. Low-cost storage service providing secure and durable storage for data archiving and backup of data that is infrequently accessed and for which retrieval times of several hours are suitable.
- AWS Identity and Access Manager (AWS IAM). Supports identity federation for delegated access to the AWS Management Console or AWS APIs, such as an Amazon S3 bucket or an Amazon DynamoDB table. By integrating on-premises identity management and AWS, customers can quickly implement single sign on (SSO), addition/deletion of users, and fine-grained AWS resource access using existing identity management solution.
- AWS Directory Service. A managed service that allows customers to connect AWS resources with an existing on-premises Microsoft Active Directory or to set up a new, stand-alone directory in the AWS Cloud.
- Integrated Resource and Deployment Management. AWS APIs allow for a wide variety of monitoring and management tools to integrate easily with AWS Cloud resources. Common tools from vendors such as Microsoft, VMware, BMC Software, Okta, RightScale, Eucalyptus, CA, Xceedium, Symantec, Racemi, and Dell already support AWS.
- AWS OpsWorks. An application management service to facilitate deploying and operating applications in the AWS Cloud or in the data center. Customers can define the application's architecture and the specification of each component, including package installation, software configuration, and resources. OpsWorks' integrates with Amazon CloudWatch as a single tool to create alarms or scale servers/instances based on CPU, memory, and load metrics in a hybrid environment.
- AWS CodeDeploy. A service to automate code deployments to instances, both in AWS and on-premises, to rapidly release new features, avoid downtime during deployment,

and handle the complexity of updating applications. It eliminates the need for error-prone manual operations, and the service scales with infrastructure so customers can easily deploy to one instance or thousands.

17.1.3 SERVICENOW

ServiceNow provides an extensive roster of integration and customization options, as highlighted in Table 16: ServiceNow Integration Highlights.

Integration	Description
Native Integration	• Altiris (version 6.5): MID Server • Google Maps: Web services • Google Custom Search: Web services • Microsoft SMS / SCCM: MID Server • Verizon eBonding: Web services
Interfaces	• Email • JDBC • JSON • LDAP • SOAP • REST API • SSO - SAML 2.0 • Digest token authentication • ODBC • Data Export • CTI • Syslog probe

Table 16: ServiceNow Integration Highlights

17.2 Customization and Personalization (8.18.2)

Utah Solicitation Number SK18008 Requirement: Page 30
8.18.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

Red River will work on a case by case basis with Purchasing Entities to determine if customization is required to meet specific needs. Once established, our technical staff, cloud service providers, and/or available knowledge based artifacts will be available to work with

Purchasing Entities to demonstrate how easily they can extend or customize as many of the cloud service providers have very extensive and configurable options as mentioned with the standard use of open APIs. For example, customers might commonly want to extend physical connectivity via dedicated, consistent, private networking between the data center and the cloud service providers they choose. With the use of these APIs, they can do it easily and quickly.

17.2.1 AppDynamics

In AppDynamics, instrumentation refers to how app agents interact with your application software to gather performance data and report it back to the AppDynamics Controller.

- Instrumenting starts with the deployment of the agents - agents ship with default instrumentation settings that cover the most common types of application frameworks and programming patterns. If your requirements are more complex, the instrumentation can be configured to customize behavior, including
  - Transaction detection rules that define entry points for business transactions.
  - Backend detection rules that define exit points for your business transactions.
  - Error detection settings that define which transactions qualify as error transactions.
  - Service endpoints to view metrics specific to services and transaction segments outside the context of a single business transaction.
  - Diagnostic data collectors for an app agent to extract additional context about a specific transaction at transaction snapshot time. You can also configure data collectors for Application Analytics.
  - Call Graph Settings to tune the amount of data the app agent collects for call graphs.
- In addition to the instrumentation configuration options covered in this topic, there are many other ways to customize AppDynamics for your environment. For more information on the items on the Configuration page, refer to the following topics:
  - "Configure Thresholds" on Transaction Thresholds.
  - "View Baselines" on Dynamic Baselines.
  - Information Points
  - Development Level Monitoring

17.2.2 AWS

☑ *Please see our response to Section 17.1 Integration (8.18.1) Subsection 17.1.2 AWS*
☑ *Please also see the entire list of services, integrations and customizations in Section 29 APPENDIX: AWS Service Description*

17.2.3 SERVICENOW – VALIDATE

ServiceNow provides a variety of ways to customize through various configurations and is dependent upon client requirements and environment. ServiceNow was built around the premise that threshold and workflows can be established to address priorities, necessary "next steps" and other configurable tracking. For example, to customize unique SLAs within the ServiceNow Service Management application, you can configure SLAs to define a set amount of time for a task to reach a certain condition, to ensure that incidents are closed or resolved according to the expectations set for customers.

- SLA definition - An SLA definition is used to create and progress SLAs, enabling you to use an SLA system for your organization's tasks.
- Configure SLA properties - You can configure the SLA engine, logging, and repair properties based on the requirements within your organization.
- SLA process example - As work is done on the relevant task, the SLA may change stage appropriately, depending on the information defined for that SLA in the relevant SLA definition.
- Add custom business rules to SLAs - You can add custom business rules to your SLAs.
- Add custom business rules to SLAs considerations - Prior adding custom business rules to the task SLA table, you must consider a few points regarding the processing and calculation of the task SLA based on your organization's needs.

18. (E) MARKETING PLAN (8.19)

18.1 Marketing Solutions (8.19.1)

Utah Solicitation Number SK18008 Requirement: Page 30
Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

Red River's goal in contract marketing is to create connections - connections facilitate conversations and conversations turn into sales opportunities for us, our CSPs and NASPO/ValuePoint. The marketing methodology, highlighted by Figure 15: Red River High-Level Marketing Approach below, is simple:

- Develop the messaging, content and creative that will fuel branding and lead generation
- Enable our sales organization and our partner community
- Execute campaigns that use a variety of marketing tools and tactics to increase awareness and drive demand
- Provide high-level air cover through advertising and media relations
- And finally nurture and qualify with a sound lead management process.

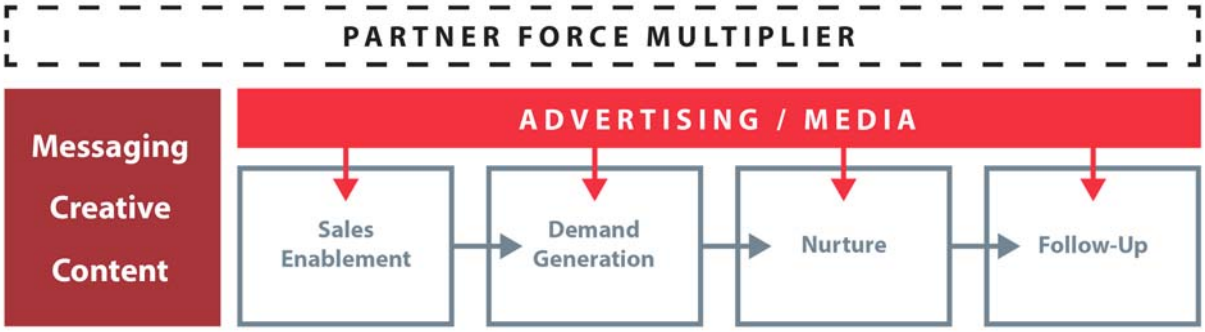


Figure 15: Red River High-Level Marketing Approach

18.1.1 DEVELOP THE MESSAGE

The process starts with message, content and creative development. For this key vehicle, Red River will:

- Develop a landing page on www.RedRiver.com to prominently feature logos and links to NASPO/ValuePoint and our CSP partners, contract resources (e.g., RFP, our response and other collateral approved by NASPO/ValuePoint for dissemination).
- Update our Contract Portfolio Guide - Figure 16: Red River Contract Portfolio Guide and Battlecard below shows the current guide – we will update the guide to verify the

NASPO/ValuePoint vehicle and opportunities is clearly identified. The guide and supporting NASPO/ValuePoint-specific material will include:

- Contract Title
- Contract Number and Formal Description
- Summary Overview of the Contract
- Cloud Solutions (CSPs and Value-Added Services)
- Detailed Contact Information
- Red River Single Point of Contact

- Create a sales battle card and data sheet – Figure 16: Red River Contract Portfolio Guide and Battlecard also includes our current Cloud Solutions Battlecard. The Battlecard is a sales-enabler, providing the information necessary for our teams to convey the right information and ask the right questions

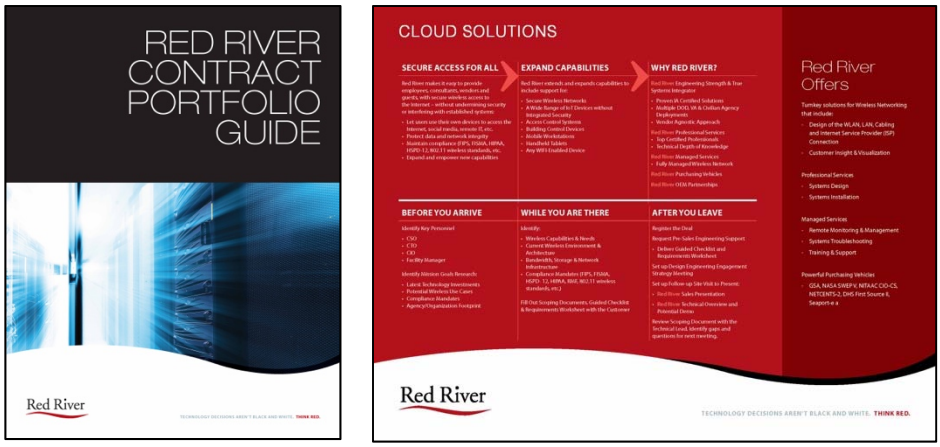


Figure 16: Red River Contract Portfolio Guide and Battlecard

18.1.2 SALES ENABLEMENT

Red River recognizes that the underlying MSA is a critical step – but not the last. Our message development is compiled to help orient our teams to the opportunities across the states. We understand the importance of working with individual states to develop the appropriate Participating Addendum that allows our team to engage with specific clients and specific opportunities. Our State, Local and Education (SLED) has representation in 47 states and we are ready to leverage our existing relationships to engage the right parties in addendum development.

In parallel to developing the state-specific vehicles, we will build and use key communication channels:

- Sales Training Video and supporting collateral (see Figure 17: Current Cloud-Focused Information and Datasheets) to demonstrate the benefits, including the incorporated terms, contract scope and pricing advantage, of the contract over alternative options, including competitive solicitations, as a more effective alternative to the cost and time associated with such alternate bids and solicitations

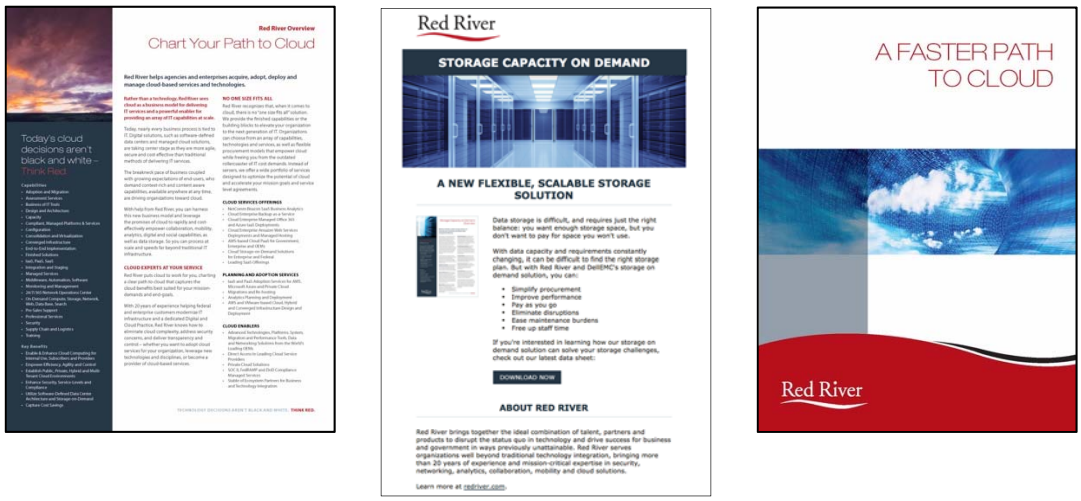


Figure 17: Current Cloud-Focused Information and Datasheets

- Internal Newsletters and employee-driven outreach
- Partner Outreach, including introductions and updates through the Newsletter Spotlight, updates to our Partner Contract Fact Sheet, and conduct interactions to seek approvals to extend potential deeper discounts to eligible participants
- Procurement workshops and roundtables in our National Sales Conference (Momentum)

18.1.3 NURTURE OPPORTUNITIES AND CAPABILITIES

Our State, Local and Education (SLED) team has representation in 47 states and we are ready to leverage our existing relationships to engage the right parties in addendum development. With our sales and partner ecosystem aligned, we are confident we can move quickly to secure the state-specific vehicles necessary to conduct direct client engagement. A key driver for finalizing those vehicles will be our commitment to direct traditional "open market" sales to the

NASPO/ValuePoint MSA, where beneficial to an eligible participant, and present the contract as our preferred acquisition vehicle.

In parallel and as Participating Addenda are being finalized, Red River will support the NASPO/ValuePoint MSA in our partner and industry ecosystems, such as:

- Technology Community - Red River is an industry leader in driving thought leadership in nationwide events, including national organizations (e.g., National Association of State Chief Information Officers/NASCIO, SuperComputing, Air Force Information Technology & Cyberpower Conferences (AFITC), and SecureWorld) and state-specific organizations (e.g., California CIO Academy, CompTIA SLED Summits, and Massachusetts Digital Government Summits)
- Procurement and Contract Management Community – Red River is an active participant in procurement best practices, including NASPO, National Coalition for Public Procurement (NCPP), Institute for Public Procurement (NIGP), or National Association of Counties (NACo)

18.1.4 Demand Generation and Follow-up

After building awareness and connections with our demand generation and advertising campaigns, Red River marketing will nurture and qualify opportunities. Like most organizations, we do this through drip email marketing, telemarketing and appointment setting. Our SLED team has deep relationships at a state level, which we will leverage as we regularly interact for on-premise infrastructure, professional and consulting services and cloud solutions. Unlike most organizations, we also have two key tools that make our nurture process unique - Red River's Innovation Center and Executive Briefing Center.

The Red River Innovation Center allows government agencies and business enterprises to push boundaries and expand capabilities without the risk, cost or complexity of adding infrastructure or staff.

Figure 18: Red River Innovation Center

Our Executive Briefing Center (under construction, due to be completed this year) provides a transformative experience that leads to new thinking and actionable plans. It connects our customers and prospects with Red River thought leaders and technology experts to discover inventive solutions that help expand capabilities, optimize technology investments and stay ahead of tomorrow's challenges.

19. (E) RELATED VALUE-ADDED SERVICES TO CLOUD SOLUTIONS (8.20)

19.1 Value-Added Services (8.20.1)

Utah Solicitation Number SK18008 Requirement: Page 30
Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

Our expertise on large-scale engagements allows us to provide value-added services for both pre- and post-implementation. Figure 19: Red River Cloud Capability Areas highlights the services we are experienced in providing in the cloud solution lifecycle.

.

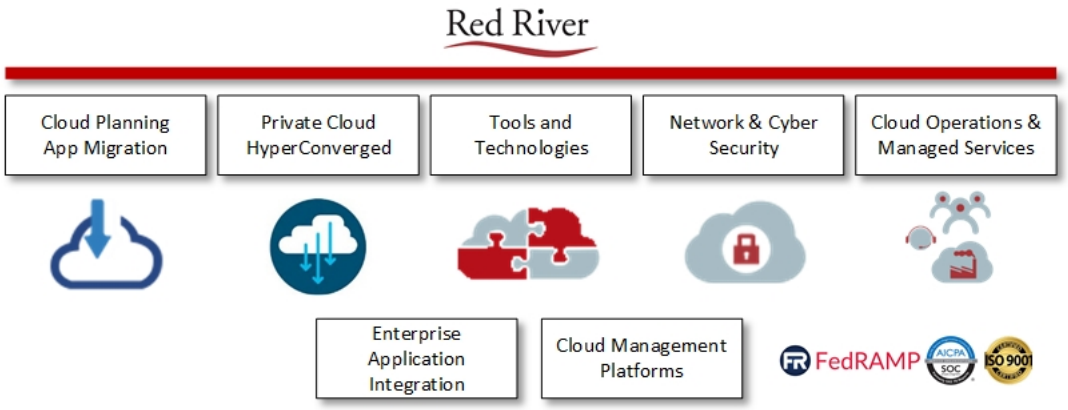


Figure 19: Red River Cloud Capability Areas

19.1.1 CLOUD VALUE-ADDED SERVICES FRAMEWORK

This proposal has focused on cloud platforms, tools and technologies - we are confident that the three CSP solutions we outline in our proposal are class leaders. This section describes the value-added services where we can offer our expertise across the lifecycle that includes the pre- and post-deployment services – cloud planning, cloud migration, application integration and managed services. We've organized the remainder of the section using the Path to Cloud framework we developed and continually refine to meet the latest industry best practices, client feedback and lessons learned.

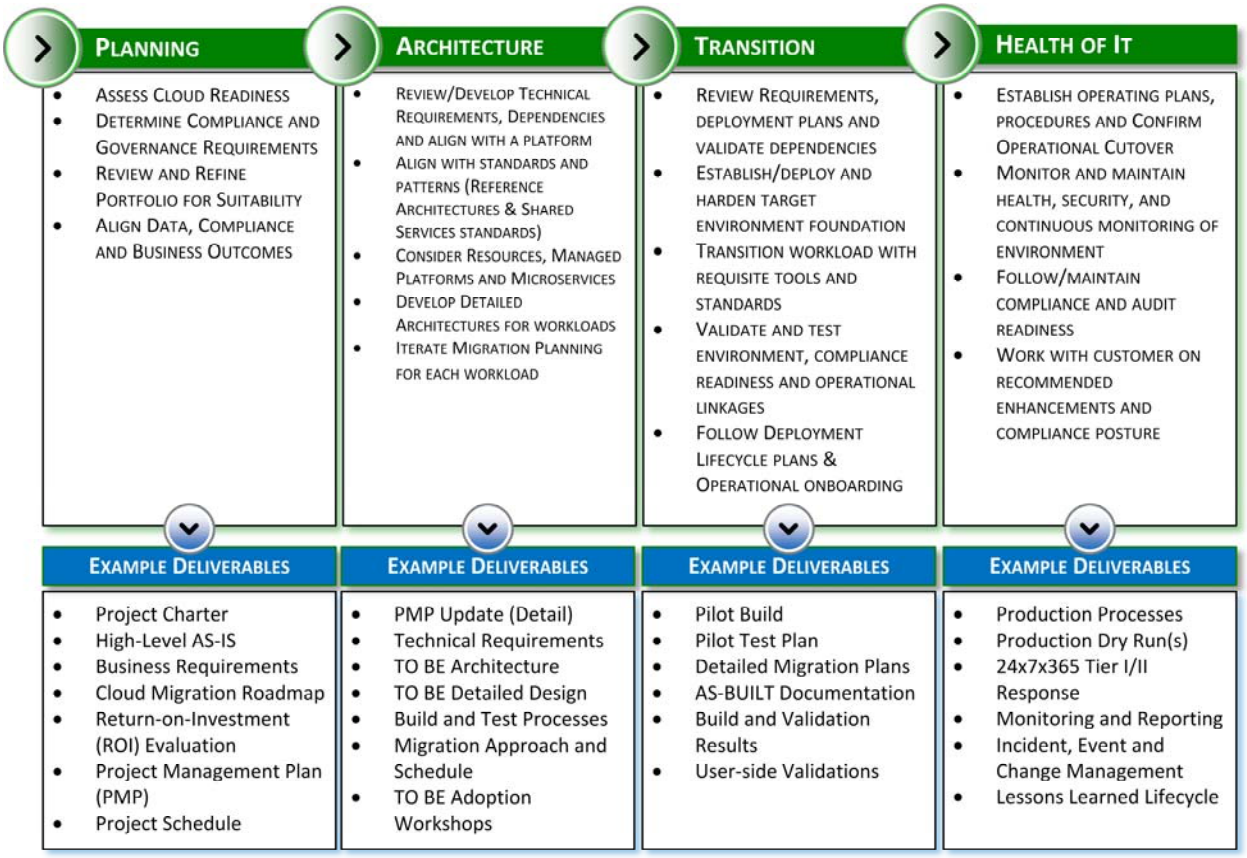


Figure 20: Path to Cloud Value-Added Services

19.1.1.1 Cloud Planning

Red River's experience in cloud solutions arrives a common set of client objectives in "cloud:"

- Cost-reduction vs. current spend
- Significant reduction or (preferably) elimination of on-premise data center footprints
- Consideration of redeploying personnel to higher value IT activities

Red River maintains a deep reserve of experienced cloud professionals for sales consultancy and "hands-on" support of client organizations that have made a cloud decision but may lack the internal capabilities to meet timeline objectives or organizations that are considering the move to cloud and request assistance in planning the effort. Our Planning step is focused on gaining a deep understanding of the current-state environment, such as existing on-premise hardware and software, contracts and licensing, security policies and stance and associated networking infrastructure. We also prefer direct stakeholder interaction, frequently through cloud adoption workshops, to elicit working knowledge of the people and processes currently in place and the level of willingness and skillset for the transition.

A current-state assessment will be focused on gathering Cloud-migration-relevant information only. The findings and the recommendations allow the population of templates to estimate the return on investment (ROI), including current-state costs (personnel, equipment, etc.), migration

expenses and timelines and future state (direct and indirect personnel costs, subscriptions services and managed services, etc.)

19.1.1.2 Cloud Architecture

The Planning stage drives the Architecture and Design step, which outlines the TO BE environment in more granular detail, such as enterprise platform options (e.g., AWS), individual cloud solution components (e.g., App Dynamics, ServiceNow), networking (e.g., Subnets, Availability Zones, Routing), access (e.g., security groups, MFA, IAM), security stance (e.g., encryption, key management) and managed services support (e.g., logging, monitoring, incident management). Figure 21: Notional Reference Architecture highlights the type of deliverable produced to demonstrate the cloud end-state.

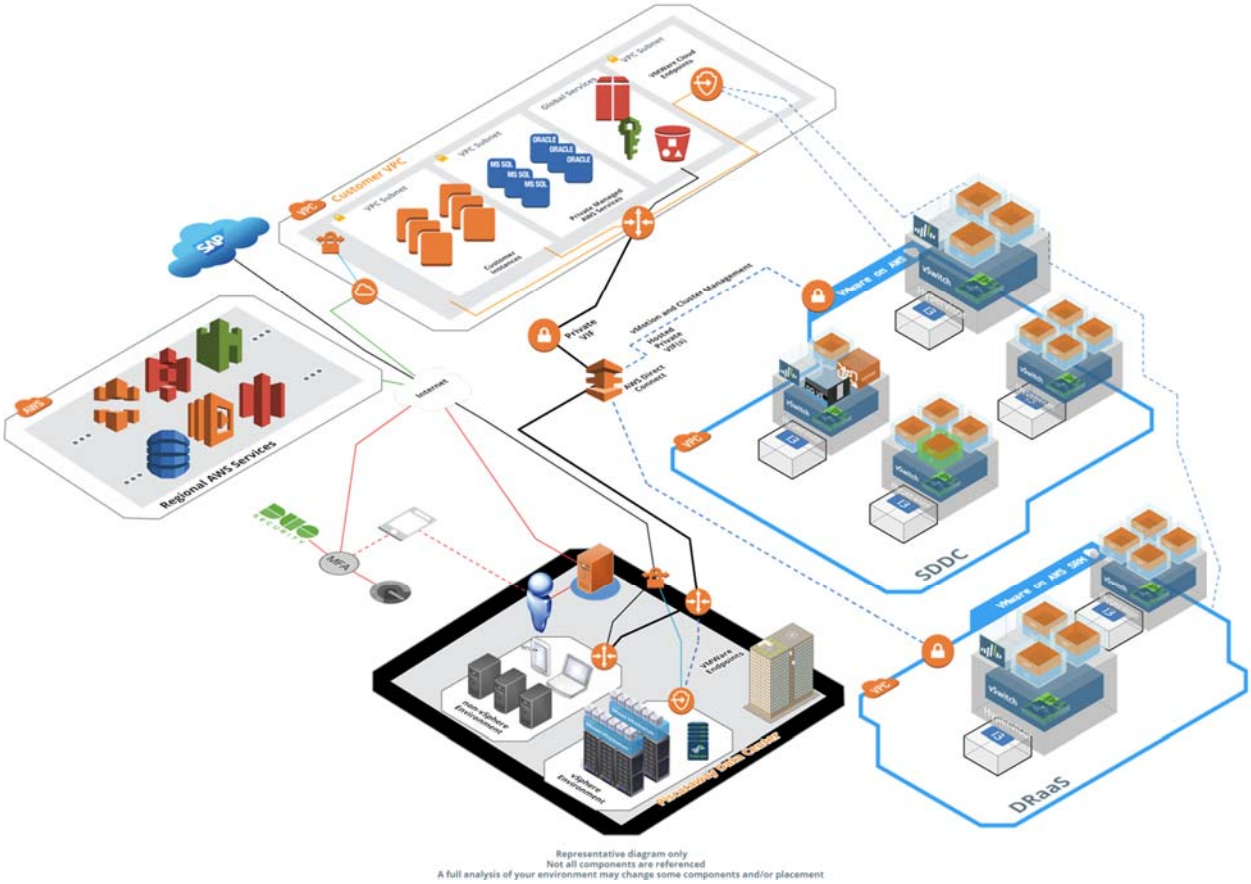


Figure 21: Notional Reference Architecture

The Architecture stage also elaborates a migration strategy that helps establish timelines, size and complexity of migration elements (if any), business criticality, stakeholder priorities and availability and risk mitigation efforts. Depending on items to be migrated to the new cloud

environment, a detailed migration plan is built for each "item" that addresses data conversion/migration/transformation, tools, test and validation, and post-migration support.

19.1.1.3 Cloud Transition

Red River has expertise in working collaboratively with both clients and target CSPs, including AWS, App Dynamics and ServiceNow, to carry out the implementation and migration strategy. We recommend the best practice of establishing the landing zone/target architecture and then conducting a pilot to vet the strategy around people, process and technology. Once we've successfully captured lessons learned and refined the approach, we can assist clients or assume lead services roles, in executing the remaining implementation and migration schedule.

This stage also initiates production plans – the development of operational processes and procedures to vet the final production cutover and verify the staff, procedures and tools are in place for "live" operation. Depending upon the strategy, Red River can support or lead efforts through this period and can prepare for concurrent migration and production support activity through a DevOps type of engagement or can support a "big-bang" cutover to Managed Services.

19.1.1.4 Cloud Health Monitoring and Operations

Client organizations can elect to conduct their own managed services, plan for direct support with the CSPs or elect to have Red River provide managed services through our U.S.-based SOC-2 and ISO 9001:2015 certified NOC. The 24/7/365 support can provide Tier 1, 2 and 3 based upon client requirements and has the certified engineers to help manage incidents, problems, events and changes in coordination with both client and CSP stakeholders as well as beyond" the specific CSP, if desired, to network infrastructure and other functions supportive or connected to cloud solutions. **Error! Reference source not found.** below is the framework for our managed services, provided as reference to the value-added services we are currently performing for clients.

Services & Tasks	Red River
Event Management • Event: A change of state which has significance for the management of a Configuration Item or IT Service. • The purpose of event management is to detect events, understand what they mean, and take any necessary action.	• Red River Monitoring and Alert Logic • Alert verification, classification, & escalation
Incident Management • Incident: An unplanned interruption to an IT Service or a reduction in the Quality of an IT Service. Failure of a Configuration Item that has not yet impacted Service is also an Incident. For example, Failure of one disk from a mirror set.	• Remote troubleshooting of support configuration items • Remote troubleshooting with AWS and OEMs

Services & Tasks	Red River
• The primary Objective of Incident Management is to return the IT Service to Users as quickly as possible.	
Problem Management • Problem: A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation. • The primary Objectives of Problem Management are to prevent Incidents from happening and to minimize the Impact of Incidents that cannot be prevented.	• Remote root cause analysis and resolution proposal • Log known errors and workarounds •
Change Management • Change: The addition, modification or removal of anything that could have an effect on IT Services. The Scope should include all IT Services, Configuration Items, Process, Documentation, etc. • The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT Services.	• Monthly server patching • Emergency patching for U.S.-cert alert vulnerabilities • Client requests for change
Request Fulfillment • Service Request: A request from a User for information, or advice, or for a Standard Change or for Access to an IT Service. For example, to reset a password, or to provide standard IT Services for a new User. Service Requests are usually handled by a Service Desk, and do not require a Request for Change (RFC) to be submitted. • Request Fulfillment: The Process responsible for managing the Lifecycle of all Service Requests.	• Requests for information about supported configuration items • Supported item performance reporting • Backup daily checks

Table 17: Sustainment Services Matrix

We have also provided an example of an SLA/SOW for a Red River Managed Services client in Section 32 APPENDIX: RRMS SLA and Agreement Sample beginning on page 249

19.1.2 Cloud Value-Added Staffing Expertise

Red River can lead or supplement client organizations with direct/dedicated staff with the requisite expertise to assist in defined domains. As highlighted in Section 17 (E) INTEGRATION AND CUSTOMIZATION (8.18) on page 114, Red River maintains capability areas in integration with our EAD, cloud-supportive network and security infrastructure with our Strategic Offerings engineering group and project management expertise in our Strategic Programs organization responsible for large-scale cloud deployments. Table 18: Value-Added Cloud Staffing Support below provides a description of the cloud-focused staffing support Red River can offer in the planning, deployment and monitoring of cloud initiatives.

Role	Senior	Mid-Level
Cloud Strategy - staff with expertise in helping senior and executive clients plan for cloud installations and migrations		
Cloud Strategist • Expertise in planning, installation, migration and ongoing operations of cloud technologies with business and technical executives • Experience in digesting industry trends and best practices to structure engagements to identify cloud cost-benefit, deployment options and schedules • Conducts stakeholder interactions with business executives to elicit objectives	• 10y in overall strategy and planning for large-scale technical engagements • 5y experience in evaluating and implementing cloud-based platforms • BS of equivalent in work experience	• N/A
Cloud Enterprise Architect • Expertise in designing cloud frameworks to industry best practices, including network configuration, cloud platform architecture (hybrid, hyper-converged, public, private), and 'as-a-service' tools (Software, Platform, Infrastructure, Storage, etc.) • Experience in digesting industry trends and best practices to structure engagements to identify cloud cost-benefit and design options, including Data Storage, Operating Systems, Virtualization, Identity Management, and Disaster Recovery • Conducts stakeholder interactions with technical executives to elicit objectives	• 10y in overall strategy and planning for large-scale technical engagements • 5y experience in evaluating and implementing cloud-based platforms • BS or equivalent in work experience	• N/A
Cloud Managed Services Architect • Expertise in identifying and developing SLAs for cloud platforms, including elicitation of unique client requirements • Experience in designing operations monitoring, problem/incident management and production support protocols to align with SLAs • Experience in digesting industry trends and best practices Hosting, Disaster Recovery, Networking, Service Desk and other infrastructure • Conducts stakeholder interactions with technical executives to elicit objectives	• 10y in overall strategy and planning for operational support of large-scale technical engagements • 3y experience in evaluating and implementing cloud-based structures • BS or equivalent in work experience	• N/A

Role	Senior	Mid-Level
Cloud Program Management – staff with expertise in building out delivery strategies and plans		
Cloud Program Manager • Planning and directing business, technical, and personnel for a diverse group of activities which include cloud platform technology improvement, engineering, applications, infrastructure installation, test and deployment. • Facilitates definition of scope, requirements, schedules and plans; Implements project plans to meet objectives; coordinates and integrates project activities, manages, leads or administers project resources; monitors project activities and resources to mitigate risk	• 8y in program/project management similar in scope and requirements • BA of equivalent in work experience • PMI PMP	• 4y in program/project management similar in scope and requirements • BA of equivalent in work experience • PMI PMP
Cloud Subject Matter Expert • Expertise in industry issues and trends in the detailed planning, implementation and dependencies in cloud migration • Assists establishing the operational and functional baseline of an organization and its organizational components and helping build a stakeholder-driven approach to cloud readiness • Coordinates resolution of complex problems and tasks, possesses ability to meet and operate under deadlines.	• 5y experience in cloud platforms • 7y experience in technical program delivery • BS in technical field, or equivalent technical experience	• 3y experience in cloud platforms • 5y experience in technical program delivery • BS in technical field, or equivalent technical experience
Cloud Technical Delivery – staff with expertise to design, develop and implement cloud platforms		
Cloud Configuration and Development Specialist • Provides technical and administrative direction for personnel performing configuration of cloud infrastructure, application migration, and post-migration engineering remediation • Plans, designs and develops technical work products for adherence to design concepts, engineering and security standards	• 4y experience in cloud configuration • 2y specific to analysis and design in a lead capacity • 6y experience in configuration management on large-scale technical projects • BS in technical field, or equivalent technical experience	• 2y experience in cloud configuration • 1y specific to analysis and design of business applications • 3y experience in configuration management on large-scale

Role	Senior	Mid-Level
		technical projects • BA in technical field, or equivalent technical experience
Cloud Network Specialist • Leads the design, configuration and implementation of networking infrastructure, including direct circuits, VPN tunnels, and MPLS technologies • Coordinates with technical resources for the alignment of network capabilities (e.g., bandwidth, volume peaks, encryption standards) with cloud platforms and cloud-hosted applications	• 3y experience in network architecture and deployment with cloud-based platforms • 1y in a lead capacity • 4y experience in network design and development • BS in technical field, or equivalent technical experience (e.g., certifications)	• 2y experience in network architecture and deployment with cloud-based platforms • 3y experience in network design and development • BS in technical field, or equivalent technical experience (e.g., certifications)
Cloud Security Specialist • Leads the design, configuration and implementation security architectures and technical components • Identifies and applies appropriate security standards, including NIST, FISMA, FIPS, IRS, HIPAA and other protocols • Identifies and applies security protocols, including identify management/authentication, encryption, intrusion and analytics	• 3y experience in security programs for cloud-based platforms • 1y specific to analysis and design of business applications in a lead capacity • 4y experience in network design and development • BS in technical field, or equivalent technical experience (e.g., certifications)	• 2y experience in network architecture and deployment with cloud-based platforms • 3y experience in network design and development • BS in technical field, or equivalent technical experience (e.g., certifications)
Cloud Analyst • Leads or supports the Cloud Program Manager and team in documenting and	• 5y experience in system development lifecycle support	• 3y experience in system development

Role	Senior	Mid-Level
executing schedule tasks, including design, development, test, training and implementation • Coordinates the elicitation and documentation of requirements, the design and development of test plans and scripts, executes test scripts, documents results and coordinates with technical staff to identify remediation options • Plans, documents and conducts training and implementation support, including documentation and delivery	• 2y specific to analysis and design in a lead capacity • BA or BS, or equivalent experience (e.g., certifications)	lifecycle support • BA or BS, or equivalent experience (e.g., certifications)
Cloud Operations and Health Monitoring – staff with expertise planning and conducting production operations and performance monitoring		
Cloud Operations Lead • Leads or supports the Cloud Program Manager and team in developing and implementing production support protocols, including O&M plans, DevOps tools and methodologies and ongoing health monitoring • Coordinates the elicitation and documentation of support requirements and SLAs • Plans and executes operational readiness activities, including coordination of client dependencies • Establishes and maintains support tools, such as ServiceNow ticketing and incident management, AppDynamics monitoring and other analytics and problem management capabilities	• 7y experience in providing production support for large-scale infrastructure and applications • 3y experience in a lead capacity of operational support or managed services • 2y experience in cloud-based platforms and technologies • BA or BS, or equivalent experience (e.g., certifications)	• 3y experience in providing production support for large-scale infrastructure and applications • 1y experience in a lead capacity of operational support or managed services • 1y experience in cloud-based platforms and technologies • BA or BS, or equivalent experience (e.g., certifications)
Cloud Operations Analyst • Assists in the planning and readiness of operational support processes • Conducts direct support (Tier I/II) for production operations, including problem,	• 3y experience in providing production support for large-scale infrastructure and applications	• 2y experience in providing production support for large-scale infrastructure

Role	Senior	Mid-Level
incident, change and fulfillment requests and management • Exercises support tools, such as ServiceNow ticketing and incident management, AppDynamics monitoring and other analytics and problem management capabilities	• 1y experience in cloud-based platforms and technologies • BA or BS, or equivalent experience (e.g., certifications)	and applications • BA or BS, or equivalent experience (e.g., certifications)

Table 18: Value-Added Cloud Staffing Support

20. (E) SUPPORTING INFRASTRUCTURE (8.22)

20.1 Infrastructure Description (8.22.1)

Utah Solicitation Number SK18008 Requirement: Page 30
8.22.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

As cloud solutions, the need for new client-specific infrastructure components is minimized if not eliminated. Our experience is that client operations may need a review network infrastructure, such as bandwidth, circuits and other components to optimize their environment for the move to cloud if entirely or mostly on-premise in current activities.

20.1.1 APPDYNAMICS

As the leader for Application Performance Management, AppDynamics delivers a cloud-based solution that enables you to quickly deliver real-time visibility with confidence. With AppDynamics SaaS, clients can focus on driving the best digital experiences for your customers while enjoying lower total costs, guaranteed availability, data security and automatic upgrades.

By delivering a cloud-based, high-performance platform, AppDynamics SaaS helps you rapidly start to ensure that every part of your environment — from software to infrastructure to business outcomes — is highly visible, optimized, and primed to drive growth. The only required infrastructure in a SaaS based model is installation of our software agent on your application, with associated costs included in the subscription model.

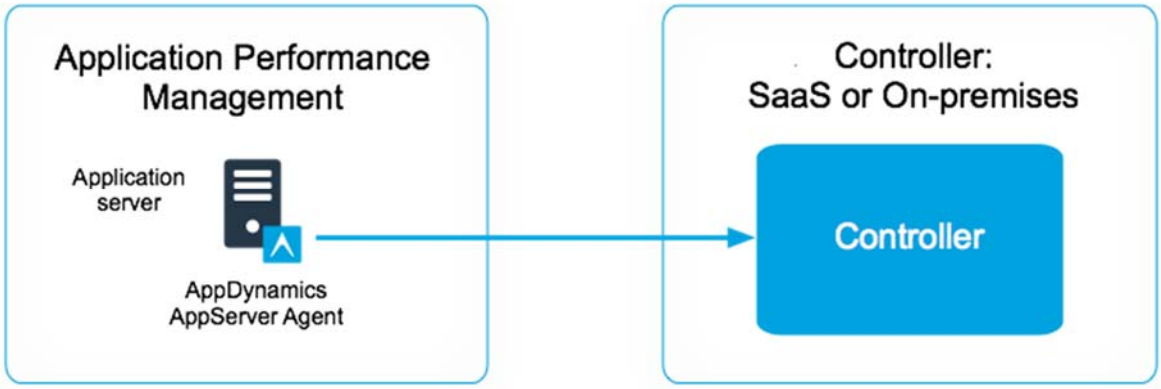


Figure 22: AppDynamics AppServer Agent

20.1.2 AWS

AWS IaaS, PaaS, and SaaS offerings are designed to be deployed such that they are accessed via client networks (e.g., client ISP to AWS).

20.1.3 SERVICENOW

ServiceNow is a cloud-based SaaS and as such, the client has access to our With AppDynamics Software-as-a-Service (SaaS), you can focus on driving the best digital experiences for your customers while enjoying lower total costs, guaranteed availability, data security and automatic upgrades. By delivering a cloud-based, high-performance platform, AppDynamics SaaS helps you rapidly start to ensure that every part of your environment — from software to infrastructure to business outcomes — is highly visible, optimized, and primed to drive growth.

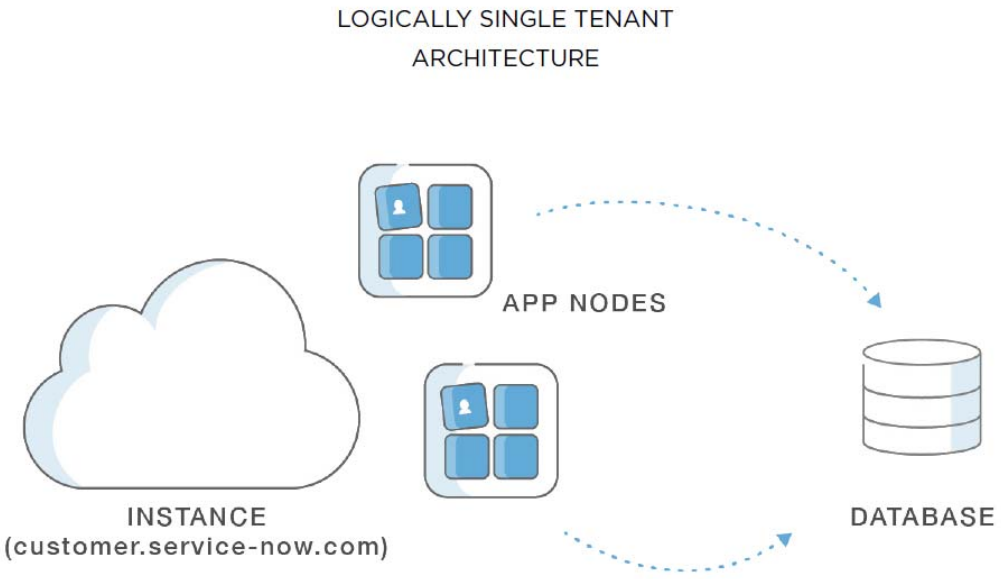


Figure 23: ServiceNow Architecture

20.2 New Infrastructure Installation (8.22.2)

Utah Solicitation Number SK18008 Requirement: Page 30 *8.22.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?*

Red River has provided CSP-specific responses below.

20.2.1 APPDYNAMICS

AppDynamics provides its software as a service (SaaS). All software components are maintained by AppDynamics consistent with terms in the SLAs.

☑ *Please refer to the following responses for additional SLA information*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.1 AppDynamics*
- *Section 21 APPENDIX: AppDynamics SLA (as of 6-29-2018)*

20.2.2 AWS

Infrastructure supporting AWS IaaS, PaaS, and SaaS offerings are maintained by AWS, with updates provided consistent with SLAs.

☑ *Please refer to the following sections for additional information on SLAs*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.2 AWS*
- *AWS SLAs in Section 22 Appendix beginning on page 158 and continuing through Section 28 Appendix*

20.2.3 SERVICENOW

ServiceNow provides its software as a service (SaaS) and its components are maintained by ServiceNow. Any updates are released in the manner and by procedures detailed in the ServiceNow SLA.

☑ *Please refer to the following sections for additional information on SLAs*
- *Section 3.6 Service Level Agreements (8.3.6) Subsection 3.6.3 ServiceNow*
- *Section 30 APPENDIX: ServiceNow Subscription Guide-SLA (as of 6-29-2018)*

21. APPENDIX: APPDYNAMICS SLA (AS OF 6-29-2018)

APPDYNAMICS SOFTWARE AS A SERVICE (SAAS) END USER LICENCE AGREEMENT TERMS

Applicable Terms:

This cover note explains which version of the End User Licence Agreement governs End User's use of the Software:

1. If End User is located in North, South or Central America, then:

(a) the **Americas End User Licence Agreement** (a copy of which is set out in **Annex A** to this note) shall apply as between AppDynamics LLC and End User; and

(b) if End User is subject to Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (**General Data Protection Regulation**) and (ii) End User collects personal data (as defined by the General Data Protection Regulation) using the Software which is stored by AppDynamics, the terms of the Data Processing Exhibit set out in **Annex B** to this cover note shall also apply.

2. If End User is located outside of North, South or Central America, the **Non-Americas End User Licence Agreement** (a copy of which is set out in **Annex C** to this note) shall apply as between AppDynamics International Ltd and End User.

Annex A

Americas End User Licence Agreement

AppDynamics LLC End User License Agreement

1. SOFTWARE LICENSE.

1.1 License Grant. This End User License Agreement (this "Agreement") between AppDynamics LLC, a Delaware limited liability company with its principal place of business located at 303 Second Street, North Tower, 8th Floor, San Francisco, CA 94107 ("AppDynamics") and the customer set forth on the Order Form (as defined below) ("End User") is effective as of the date the applicable Order Form is executed or the date this Agreement is referenced by the applicable purchase order (the "Effective Date"). This Agreement shall govern each order form, sales quotation, proposal, purchase order or other ordering document that references this Agreement (each an "Order Form"). Each Order Form will form part of this Agreement. Subject to the terms and conditions of this Agreement, AppDynamics hereby grants to End User, during the License Term (as defined below), a non-exclusive, non-transferable, non-sublicensable right and license to use AppDynamics' software product, including one Controller (as defined in Exhibit B), as designated in the Order Form(s) (the "Software") for internal business purposes only for the quantity of units in the Order Form. For purposes hereof, the "License Term" begins on the date AppDynamics delivers the Software license keys to End User and extends for the period specified in the applicable Order Form (unless earlier terminated in accordance with this Agreement). This Agreement supersedes any other agreement (including any click-through or electronic agreements within the Software) between AppDynamics and End User with respect to the Software. Any references in the Order Form to an "agreement" or "EULA" or other similar term shall be deemed to refer to this Agreement.

1.2 Restrictions on Use. AppDynamics Test & Dev Edition licenses shall only be used in test-only non-production environments. Except as otherwise expressly provided in this Agreement, End User shall not (and shall not permit any third party to): (a) sublicense, sell, resell, transfer, assign, distribute, share, lease, make any external commercial use of, outsource, use on a timeshare or service bureau basis, or use in an application service provider or managed service provider environment, or otherwise generate income from the Software; (b) copy the Software onto any public or distributed network, except for secure cloud computing environments; (c) cause the decompiling, disassembly, or reverse engineering of any portion of the Software, or attempt to discover any source code or other operational mechanisms of the Software (except where such restriction is expressly prohibited by law without the possibility of waiver, and then only upon prior written notice to AppDynamics); (d) modify, adapt, translate or create derivative works based on all or any part of the Software; (e) use any Third Party Software (as defined below) provided with the Software other than with the Software; (f) modify any proprietary rights notices that appear in the Software or components thereof; (g) publish the results of any benchmarking tests run on any Third Party Software; (h) use any Software in violation of any applicable laws and regulations; (i) use the Software in support of any nuclear proliferation, chemical weapon, biological weapon or missile proliferation activity; (j) configure the Software to collect any (1) social security numbers or other government-issued identification numbers, (2) passwords or other authentication credentials, (3) health information, biometric data, genetic data, or payment/financial information, (4) any data relating to a person under the age of 13 years old, or (5) any other data that is subject to regulatory or contractual handling requirements (e.g., PCI, HIPAA, or state and federal data security laws) (collectively, "Prohibited Data"); or (k) use the Software to (1) store, download or transmit infringing, libelous, or otherwise unlawful or tortious material, or malicious code or malware, or (2) engage in phishing, spamming, denial-of-service attacks or other fraudulent or criminal activity, (3) interfere with or disrupt the integrity or performance of third party systems, or the Software or data contained therein, or (4) attempt to gain unauthorized access to the Software or AppDynamics' systems or networks, or (5) perform, or engage any third party to perform, authenticated or unauthenticated penetration testing, vulnerability assessments or other security assessments on the SaaS version of the Software. End User shall not export or re-export, directly or indirectly, any Software or technical data or any copy, portions or direct product thereof (i) in violation of any applicable laws and regulations, (ii) to any country for which the United States or any other government, or any agency thereof, at the time of export requires an export license or other governmental approval, including Cuba, Libya, North Korea, Iran, Iraq, or Rwanda or any other Group D:1 or E:2 country (or to a national or resident thereof) specified in the then current Supplement No. 1 to part 740 of the U.S. Export Administration Regulations (or any successor supplement or regulations, without first obtaining such license or approval) or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Denial Orders. End User shall, at its own expense, obtain all necessary customs, import, or other governmental authorizations and approvals.

1.3 Evaluation Use. If End User accessed any software provided by AppDynamics pursuant to a no-fee or beta evaluation ("Beta Software"), then the License Term is for the period enabled by the license key for the Beta Software. AppDynamics shall have the right to terminate, downgrade, limit or otherwise modify the Beta Software at any time without notice, and no warranty, indemnity, availability, Maintenance or Support obligations of AppDynamics will apply to Beta Software. End User may use the number and type of licenses enabled by End User's specific license key. End User agrees to provide feedback related to the Beta Software as reasonably requested by AppDynamics. End User grants to AppDynamics, without charge, the fully paid-up, perpetual, sublicensable right to exploit such feedback for any purpose. The provision of Beta Software is not a guarantee of future product features or the availability of

any future product and should not be relied upon in making any purchasing decisions.

1.4 AFFILIATE USE. For purposes hereof, "Affiliate" means, in relation to a party, any entity that directly or indirectly controls, is controlled by, or is under direct or indirect common control with such party, or which is a wholly owned subsidiary of such party, where "control" means owning, directly or indirectly, at least fifty-one percent (51%) of the equity securities or equity interests of such entity.

(a) End User Affiliates will have the right to make purchases pursuant to this Agreement by executing an Order Form (or issuing a purchase order referencing an Order Form) and agreeing to be bound by this Agreement. Where an Affiliate makes a purchase pursuant to this Agreement, references to each party in the Agreement shall be read as references to the Affiliate of each party stated on the Order Form, except that such End User Affiliate shall not receive the benefit of the previous sentence with respect to its own affiliates. If an End User Affiliate purchases under this Agreement, then a separate Agreement will be deemed made between AppDynamics (or its Affiliate, as applicable) and such End User Affiliate.

(b) End User may also permit Affiliates to use the Software provided that (i) End User shall procure that its Affiliates comply with the terms of this Agreement, and End User shall remain liable for all acts and omissions of its Affiliates; (ii) End User represents that it can bind its Affiliates to the applicable Order Form and this Agreement; (iii) only End User may bring actions against AppDynamics with respect to any losses, damage or liabilities suffered or incurred by any Affiliate caused by the Software; and (iv) the exclusions and limitations of liability in this Agreement will apply to End User and End User Affiliates as a whole, so that they apply to all liabilities incurred under or in connection with this Agreement by AppDynamics to End User and End User Affiliates in aggregate.

1.5 MAINTENANCE AND SUPPORT. "Support" is defined as AppDynamics' obligations to respond to support requests as described in Exhibit A (Support). "Maintenance" means AppDynamics' obligations related to error resolution, bug fixes and the provision of updates and upgrades made generally commercially available by AppDynamics in its sole discretion, all as described in the Exhibit A (Support). Subject to End User's payment of the fees set forth in the applicable Order Form(s), AppDynamics will (a) provide Maintenance and Support for the Software, and (b) solely if End User has purchased access to the software-as-a-service version of the Software, make the Software available to End User in accordance with Exhibit B (Availability). For time-limited licenses for the Software (as set forth in an Order Form, "Subscription Licenses"), the fees for Maintenance and Support are included in the fees for the Software. For perpetual licenses, (i) AppDynamics shall invoice End User the applicable fees for Maintenance and Support ("Maintenance and Support Fees") upon execution of the Order Form, and (ii) subject to payment of the Maintenance and Support Fees, AppDynamics will provide Support for the Maintenance and Support period set forth in the Order Form, as it may be renewed (the "Maintenance and Support Term"). If Maintenance and Support terminates with respect to any perpetual licenses, and End User is in good standing under this Agreement, then End User may reinstate Maintenance and Support on payment of the cumulative Maintenance and Support Fees applicable for the period during which Maintenance and Support lapsed, plus Maintenance and Support Fees for the reinstated Maintenance and Support Term. Notwithstanding anything herein to the contrary, if End User receives Support from an authorized partner of AppDynamics ("Partner"), then the support terms agreed upon by End User and such Partner shall govern in lieu of those set forth in Exhibit A, and AppDynamics shall have no support obligations to End User.

1.6 SERVICES. Subject to the terms hereof, AppDynamics will provide the training, enablement and/or other services described in an Order Form (or statement of work referencing this Agreement), if any ("Services"). The license in Section 1.1 applies to any educational, training and other informational materials resulting from the Services. All Services will be rendered on a time and materials basis. AppDynamics will not exceed the total time purchased without prior written approval from End User. If the Services purchased have been consumed, AppDynamics will stop the Services until additional Services have been purchased. If not used, pre-purchased Services and expenses expire twelve (12) months after the date purchased (unless otherwise set forth in the applicable Order Form). End User agrees to provide reasonable cooperation and information as necessary to permit AppDynamics to perform the Services. End User will reimburse AppDynamics for travel and expenses (at cost) incurred in connection with the Services (if any) by the Invoice Due Date (as defined below). Services will be performed on business days (a business day means Monday through Friday, excluding national holidays, during working hours, in the location where the Services are delivered). Saturday Services, and hours worked during the week that exceed the local working hours in a week, will be charged at the agreed rate x 1.5. Services performed on Sundays or national holidays will be charged at 2 x the agreed rate. If End User cancels or delays any scheduled Services less than ten (10) business days before the start date of such Services, then AppDynamics will deduct from End User's account (or End User will pay for) the amount of Services that were scheduled in any of the ten (10) business days following the date of cancellation (or notification of the delay, as applicable), and End User will fully reimburse AppDynamics for any reasonable travel and expenses incurred by AppDynamics for such Services (and for any Services rescheduled by End User) for which AppDynamics is unable to obtain a refund. During the License Term (for Subscription Licenses) or during the Maintenance and Support Term (for perpetual licenses), and in each case for a period of twelve (12) months thereafter, without AppDynamics' prior written approval, End User will not solicit for employment

or consultancy any AppDynamics' employees who participated in the performance of Services.

2. FEES.

2.1 PRICING. End User will be invoiced for those amounts and at those prices set forth in an Order Form (an "Invoice"). Fees do not include any customization of the Software (nor support for any such customizations, unless otherwise agreed in writing). If End User's usage of the Software is in excess of those amounts set forth in the Order Form, End User may be billed for those overages. If AppDynamics believes in good faith that End User's usage of the Software exceeds that set forth on the applicable Order Form, for on-premises deployments, End User agrees to report to AppDynamics (or allow AppDynamics to audit) the quantity of Software license units used by End User, upon at least three (3) business days' notice. AppDynamics may monitor at any time the quantity of Software license units used by End User for SaaS deployments of the Software. End User acknowledges that purchases made under this Agreement are neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public comments made by AppDynamics regarding future functionality or features.

2.2 PAYMENTS. End User shall pay Invoices within thirty (30) days of the invoice date (the "Invoice Due Date"). All payment obligations are non-cancelable and all amounts paid are non-refundable, except (a) for amounts paid in error that are not actually due under this Agreement, and (b) as set forth in Sections 6.1 and 7.1. The fees paid by End User are exclusive of all taxes, levies, or duties imposed by taxing authorities, if any, and End User shall be responsible for payment of all such taxes, levies, or duties, excluding taxes based on AppDynamics' income. AppDynamics shall have no responsibility for any Invoices that are not received due to inaccurate or missing information provided by End User. End User shall pay interest on all payments not received by the Invoice Due Date at a rate of one percent (1%) per month or the maximum amount allowed by law, whichever is lesser. All amounts due under this Agreement shall be paid by End User in full without any set-off, counterclaim, deduction or withholding (other than any deduction or withholding of tax as required by law). If requested by AppDynamics, End User will obtain and furnish to AppDynamics tax receipts or other certificates issued by the competent taxation office showing the payments of the withholding tax within a reasonable time after payment. Following notice, AppDynamics shall be entitled to suspend End User's access to the Software if payments are not received within thirty (30) days of the Invoice Due Date. Notwithstanding anything herein to the contrary, if End User makes its payments pursuant to this Agreement to a Partner, then the payment terms agreed by End User and such Partner shall govern to the extent anything in this Section 2 conflicts with such Partner payment terms.

3. CONFIDENTIALITY

3.1 SCOPE AND RESTRICTIONS. "Confidential Information" means all information of a party ("Disclosing Party") disclosed to the other party ("Receiving Party") that is designated in writing or identified as confidential at the time of disclosure or should be reasonably known by the Receiving Party to be confidential due to the nature of the information disclosed and the circumstances surrounding the disclosure. The terms of this Agreement, the Software, pricing, and any technical or other documentation and communications relating to the Software, installation, Maintenance and Support and Services, logins, passwords and other access codes and any and all information regarding AppDynamics' business, products and services are the Confidential Information of AppDynamics. The Receiving Party will: (i) not use the Disclosing Party's Confidential Information for any purpose outside of this Agreement; (ii) not disclose such Confidential Information to any person or entity, other than its affiliates, employees, consultants, agents and professional advisers who have a "need to know" for the Receiving Party to exercise its rights or perform its obligations hereunder, provided that such employees, consultants, and agents are bound by agreements or, in the case of professional advisers, ethical duties respecting such Confidential Information in accordance with the terms of this Section 3; and (iii) use reasonable measures to protect the confidentiality of such Confidential Information. If the Receiving Party is required by applicable law or court order to make any disclosure of such Confidential Information, it will first give written notice of such requirement to the Disclosing Party, and, to the extent within its control, permit the Disclosing Party to intervene in any relevant proceedings to protect its interests in its Confidential Information, and provide full cooperation to the Disclosing Party in seeking to obtain such protection. Further, this Section 3 will not apply to information that the Receiving Party can document: (i) was rightfully in its possession or known to it prior to receipt without any restriction on its disclosure; (ii) is or has become public knowledge or publicly available through no fault of the Receiving Party; (iii) is rightfully obtained by the Receiving Party from a third party without breach of any confidentiality obligation; or (iv) is independently developed by employees of the Receiving Party who had no access to such information.

3.2 EQUITABLE RELIEF. The Receiving Party acknowledges that unauthorized disclosure of the Disclosing Party's Confidential Information could cause substantial harm to the Disclosing Party for which damages alone might not be a sufficient remedy and, therefore, that upon any such disclosure by the Receiving Party, the Disclosing Party will be entitled to seek appropriate equitable relief in addition to whatever other remedies it might have at law or equity.

4. PROPRIETARY RIGHTS. AppDynamics and its suppliers shall retain all intellectual property rights in and to the Software and the results of any Services. End User acknowledges that the rights granted under this Agreement do not provide End User with title to or ownership of the Software. Certain "free" or "open source"

based software (the "FOSS Software") and third party software included with the Software (the "Third Party Software") is shipped with the Software but is not considered part of the Software hereunder. A list of the FOSS Software and Third Party Software is at https://docs.appdynamics.com/display/DASH/Legal+Notices. End User's use of such FOSS Software is subject to the terms of the licenses set forth on such webpage. With respect to Third Party Software included with the Software, such Third Party Software suppliers are third party beneficiaries of this Agreement. The Software and Third Party Software may only be used by End User as prescribed by the AppDynamics documentation located at http://docs.appdynamics.com (as it may be updated from time to time, the "Documentation").

5. TERM AND TERMINATION. The term of this Agreement begins on the Effective Date and will remain in effect until all Subscription Licenses (and Maintenance and Support Terms, if applicable) expire or until this Agreement is otherwise terminated in accordance with the terms hereof, whichever occurs first (the "Term"). This Agreement may be renewed at any time by execution of an Order Form referencing this Agreement, and any such renewal will be deemed part of the "Term" hereunder. If either party commits a material breach of this Agreement, and such breach has not been cured within thirty (30) days after receipt of written notice thereof, the non-breaching party may terminate this Agreement, except that AppDynamics may immediately terminate this Agreement and/or End User's license to the Software upon End User's breach of Section 1.2. Either party may also terminate this Agreement upon written notice if the other party suspends payment of its debts or experiences any other insolvency or bankruptcy-type event. Upon expiration or termination of this Agreement for any reason, (i) with respect to Subscription Licenses, all rights granted to End User shall terminate and End User shall destroy any copies of the Software and Documentation within End User's possession and control; (ii) with respect to perpetual licenses, these will survive termination of this Agreement unless AppDynamics terminates the Agreement for End User's breach of this Agreement in which case all rights granted to End User shall terminate and End User shall destroy any copies of the Software and Documentation within End User's possession and control; and (iii) each Receiving Party will return or destroy, at the Disclosing Party's option, the Disclosing Party's Confidential Information in the Receiving Party's possession or control. All fees that have accrued as of such expiration or termination, and Sections 1.2, 1.3, 1.4, 2, 3, **4**, 5, 6.2 and 7 through 12, will survive any expiration or termination hereof.

6. WARRANTIES.

6.1 LIMITED WARRANTY. AppDynamics warrants that during the first thirty (30) days following the date the Software is purchased, the Software will, in all material respects, conform to the functionality described in the then-current Documentation for the applicable Software version. AppDynamics' sole and exclusive obligation, and End User's sole and exclusive remedy, for a breach of this warranty shall be that AppDynamics shall be required to use commercially reasonable efforts to repair or replace the Software to conform in all material respects to the Documentation, and if AppDynamics is unable to materially restore such functionality within thirty (30) days from the date of written notice of such breach, End User shall be entitled to terminate the license to the affected Software upon written notice and AppDynamics shall promptly provide a pro-rata refund of the Software license fees (or Maintenance and Support Fees, for perpetual licenses) that have been paid in advance for the remainder of the License Term for the applicable Software (beginning on the date of termination). End User must notify AppDynamics in writing of any warranty breaches within such warranty period, and End User must have installed and configured the Software in accordance with the Documentation to be eligible for the foregoing remedy.

6.2 WARRANTY DISCLAIMER. EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION 6, ALL SOFTWARE, DOCUMENTATION, MAINTENANCE AND SUPPORT AND SERVICES ARE PROVIDED "AS IS" AND APPDYNAMICS AND ITS SUPPLIERS EXPRESSLY DISCLAIM ANY AND ALL OTHER REPRESENTATIONS AND WARRANTIES, EITHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT THERETO, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, OR THE CONTINUOUS, UNINTERRUPTED, ERROR-FREE, VIRUS-FREE, OR SECURE ACCESS TO OR OPERATION OF THE SOFTWARE. APPDYNAMICS EXPRESSLY DISCLAIMS ANY WARRANTY AS TO THE ACCURACY OR COMPLETENESS OF ANY INFORMATION OR DATA ACCESSED OR USED IN CONNECTION WITH THE SOFTWARE, DOCUMENTATION, MAINTENANCE AND SUPPORT, OR SERVICES OR THAT THE SOFTWARE WILL BE COMPATIBLE OR WORK WITH ANY END USER OR THIRD PARTY SOFTWARE OR HARDWARE. Each party acknowledges that, in entering into this Agreement, it has not relied on, and shall have no right or remedy in respect of, any statement, representation, assurance or warranty (whether made negligently or innocently) other than as expressly set out in this Agreement. AppDynamics is not responsible for any delays, delivery failures, or any other loss or damage resulting from the transfer of data over communications networks and facilities, including the Internet, and End User acknowledges that the Software and Documentation may be subject to limitations, delays and other problems inherent in the use of such communications facilities. The Software is not fault-tolerant and is not designed or intended for use in hazardous environments, including without limitation, in the operation of aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles or weaponry systems, or any other application in which failure of the Software could lead to death or serious bodily injury of a person, or to severe physical or environmental damage (each, a "High Risk Use"). AppDynamics expressly disclaims any express or implied

warranty or representation of fitness for High Risk Use. AppDynamics shall not be liable to End User for any loss, damage or harm suffered by End User that is directly or indirectly caused by End User's unauthorized use of the Software to process Prohibited Data.

7. INDEMNIFICATION.

7.1 BY APPDYNAMICS. AppDynamics agrees at its expense to defend End User against (or, at AppDynamics' option, settle), any third party claim to the extent such claim alleges that the Software infringes or misappropriates any patent, copyright, trademark or trade secret of a third party, and AppDynamics shall pay all costs and damages finally awarded against End User by a court of competent jurisdiction as a result of any such claim. In the event that the use of the Software is, or in AppDynamics' sole opinion is likely to become, subject to such a claim, AppDynamics, at its option and expense, may (a) replace the applicable Software with functionally equivalent non-infringing technology, (b) obtain a license for End User's continued use of the applicable Software, or (c) terminate the license and provide a pro-rata refund of the Software license fees (or Maintenance and Support Fees, for perpetual licenses) that have been paid in advance for the remainder of the License Term for the applicable Software (beginning on the date of termination). The foregoing indemnification obligation of AppDynamics will not apply: (1) if the Software is modified by End User or its agent; (2) if the Software is combined with other non-AppDynamics products, applications, or processes, but solely to the extent the alleged infringement is caused by such combination; or (3) to any unauthorized use of the Software. The foregoing shall be End User's sole remedy with respect to any claim of infringement of third party intellectual property rights.

7.2 BY END USER. End User agrees to defend, at its expense, AppDynamics and its affiliates, its suppliers and its resellers against any third party claim to the extent such claim arises from or is made in connection with End User's breach of Section 1 or End User's negligence or willful misconduct, and End User shall pay all costs and damages finally awarded against AppDynamics by a court of competent jurisdiction as a result of any such claim.

7.3 INDEMNIFICATION REQUIREMENTS. The following are conditions to any claim for indemnification under this Section 7. The indemnified party must promptly provide the indemnifying party with notice of any claim that the indemnified party believes is within the scope of the obligation to indemnify, provided, however, that the failure to provide such notice shall not relieve the indemnifying party of its obligations under this Section 7, except to the extent that such failure materially prejudices the indemnifying party's defense of such claim. The indemnified party may, at its own expense, assist in the defense if it so chooses, but the indemnifying party shall control the defense and all negotiations related to the settlement of any such claim. Any such settlement intended to bind either party shall not be final without the other party's written consent, which consent shall not be unreasonably withheld, conditioned or delayed; provided, however, that End User's consent shall not be required when AppDynamics is the indemnifying party if the settlement involves only the payment of money by AppDynamics.

8. LIMITATION OF LIABILITY. The limits below will not apply to the extent prohibited by applicable law.

8.1 EXCEPT FOR LIABILITY ARISING OUT OF END USER'S BREACH OF SECTION 1.2 (RESTRICTIONS ON USE), IN NO EVENT SHALL EITHER PARTY BE LIABLE UNDER THIS AGREEMENT FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING DAMAGES FOR LOSS OF REVENUES OR PROFITS, LOSS OF USE, BUSINESS INTERRUPTION, OR LOSS OF DATA, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

8.2 EXCEPT FOR LIABILITY ARISING OUT OF END USER'S BREACH OF SECTION 1.2 (RESTRICTIONS ON USE), NEITHER PARTY'S LIABILITY FOR ANY DAMAGES (WHETHER FOR BREACH OF CONTRACT, MISREPRESENTATIONS, NEGLIGENCE, STRICT LIABILITY, OTHER TORTS OR OTHERWISE) UNDER THIS AGREEMENT SHALL EXCEED AN AMOUNT EQUAL TO THE TOTAL FEES PAID (PLUS FEES PAYABLE) TO APPDYNAMICS DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE CLAIM GIVING RISE TO SUCH DAMAGES. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY.

9. FORCE MAJEURE. Except for payment obligations, neither party hereto will be liable for defaults or delays due to acts of God or the public enemy, acts or demands of any government or governmental agency, fires, earthquakes, floods, other natural disasters, accidents, or other unforeseeable causes beyond its reasonable control and not due to its fault or negligence.

10. DATA COLLECTION. End User acknowledges that AppDynamics' application server and machine software agents (the "Agents") collect metrics that relate to the performance, health and resource of an application, its components (transactions, code libraries) and related infrastructure (nodes, tiers) that service those components. In addition, AppDynamics collects metrics on End Users' activities, such as web pages visited, length of visit, and which features of the Software an End User uses. If End User provides AppDynamics with any personally identifiable information ("personal data"), End User represents and warrants that such information has been collected by End User in accordance with the provisions of all applicable data protection legislation and that End User has all right and consents necessary to provide such personal data to AppDynamics. End User will indemnify AppDynamics for reasonable costs and other amounts that AppDynamics may incur relating to any breach of this Section.

11. US GOVERNMENT MATTERS. As defined in FAR section 2.101, the Software and Documentation are "commercial items" and according to DFAR section 252.227 7014(a)(1) and (5) are deemed to be "commercial computer software" and "commercial computer software documentation." Consistent with DFAR section 227.7202 and FAR section 12.212, any use modification, reproduction, release, performance, display, or disclosure of such commercial software or commercial software documentation by the U.S. Government will be governed solely by the terms of this Agreement and will be prohibited except to the extent expressly permitted by the terms of this Agreement.

12. MISCELLANEOUS. This Agreement shall be governed by and construed under the laws of the State of California, U.S.A. The parties consent to the exclusive jurisdiction and venue of the courts located in and serving San Francisco, California. Failure by either Party to exercise any of its rights under, or to enforce any provision of, this Agreement will not be deemed a waiver or forfeiture of such rights or ability to enforce such provision. If any provision of this Agreement is held by a court of competent jurisdiction to be illegal, invalid or unenforceable, such provision will be amended to achieve as nearly as possible the same economic effect of the original provision and the remainder of this Agreement will remain in full force and effect. This Agreement and its exhibits, together with the Order Form(s) and any statements of work incorporating this Agreement, if applicable, represent the entire agreement between the parties and supersede any previous or contemporaneous oral or written agreements or communications regarding the subject matter of this Agreement. The person signing or otherwise accepting this Agreement for each party represents that s/he is duly authorized by all necessary and appropriate corporate action to enter this Agreement. Any modification to this Agreement must be in writing and signed by a duly authorized signatory of both parties and no previous, contemporaneous or future oral statements will be deemed to modify this Agreement. Neither the Uniform Commercial Code (UCC) nor the Uniform Computer Information Transactions Act (UCITA) will apply to this Agreement. This Agreement shall control over additional or different terms of any purchase order, confirmation, invoice, statement of work or similar document (other than an AppDynamics Order Form, which will take precedence), even if accepted in writing by both parties, and waivers and amendments to this Agreement shall be effective only if made by non-pre-printed agreements clearly understood by both parties to be an amendment or waiver to this Agreement. For purposes of this Agreement, "including" means "including without limitation." The rights and remedies of the parties hereunder will be deemed cumulative and not exclusive of any other right or remedy conferred by this Agreement or by law or equity. No joint venture, partnership, employment, or agency relationship exists between the parties as a result of this Agreement or use of the Software. AppDynamics reserves the right to perform its obligations from locations and/or through use of affiliates and subcontractors, worldwide, provided that AppDynamics will be responsible for such parties. End User may not assign this Agreement without the prior written approval of AppDynamics and any purported assignment in violation of this section shall be void; AppDynamics may assign, transfer or subcontract this Agreement in whole or in part. Upon any assignment of this Agreement by End User that is approved by AppDynamics, any licenses that contain an "unlimited" aspect will, with respect to End User or the successor entity, as applicable, be capped at the number of authorized Software units in use immediately prior to such assignment. End User agrees that AppDynamics may refer to End User by its trade name and logo, and may briefly describe End User's business, in AppDynamics' marketing materials and website. AppDynamics may give notice to End User by electronic mail to End User's email address on record in End User's account information, or by written communication sent by nationally recognized overnight delivery service to End User's address on record in End User's account information. End User may give notice to AppDynamics at any time by any letter delivered by nationally recognized overnight delivery service or first class postage prepaid mail to AppDynamics at the following address or such other address as may be notified to End User from time to time: AppDynamics, 303 Second Street, North Tower, 8th Floor, San Francisco, CA 94107, Attn: Legal Department. Notice under this Agreement shall be deemed given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by email; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested.

EXHIBIT A
ENTERPRISE SUPPORT

GENERAL REQUIREMENTS. AppDynamics will provide access to a ticketing system that will be available twenty-four (24) hours per day, seven (7) days per week. The ticketing system will be maintained by qualified support specialists, who shall use commercially reasonable efforts to provide technical support regarding the Software.

HOURS OF OPERATION. Support is available twenty-four (24) hours per day, seven (7) days per week.

ERROR CLASSIFICATION. Any reported errors are classified in the following manner, in each case when caused by the Software:

Error Classification	Criteria
Urgent	End User production application is down or there is a major malfunction, resulting in a business revenue loss and impacting the End User application functionality for a majority of users.
High	Critical loss of End User application functionality or performance, impacting the application functionality for a high number of users.
Normal	Moderate loss of End User application functionality or performance, impacting multiple users.
Low	Minor loss of End User application functionality or product feature in question.

ERROR DEFINITION. An "error" means a reproducible malfunction in the Software that is reported by End User through AppDynamics' ticketing system that prevents the Software from performing in accordance with the operating specifications described in the then-current Documentation.

AUTHORIZED SUPPORT CONTACTS. Maintenance and Support will be provided solely to End User's designated support contacts. The Order Form may indicate a maximum number of designated support contacts for End User's service level. End User will provide its designated support contacts, including its primary email address.

END USER'S OBLIGATION TO ASSIST. If End User reports a purported error in the Software to AppDynamics, AppDynamics' ticketing system will request the following minimum information:

- A general description of the operating environment
- A list of all hardware components, operating systems and networks
- A reproducible test case
- Any log files, trace and systems files

End User's failure to provide this information may prevent or significantly delay AppDynamics' ability to identify and fix the reported error. AppDynamics' time to respond to any error will begin when AppDynamics has received all requested information from the End User and is able to reproduce the error.

ERROR RESOLUTION. If AppDynamics determines there is an error in the Software, AppDynamics may, at its sole option, repair that error in the version of the Software that End User is currently using or instruct End User to install a newer version of the Software with that error repaired. AppDynamics reserves the right to provide End User with a workaround in lieu of fixing an error.

SOFTWARE UPDATES AND UPGRADES. End User must be current on fees in order to receive access to Maintenance.

RESPONSE TIME. AppDynamics shall respond to error tickets in accordance with the tables set forth below. AppDynamics will use reasonable means to repair the error and keep End User informed of progress. AppDynamics makes no representations as to when a full resolution of the error may be made.

Error	Initial Response and Acknowledgement	Manager Escalation	VP Escalation	Email Status Updates for Open Cases
Urgent	1 Hour	1 Business Day	1 Week	Daily
High	6 Hours	1 Week	2 Weeks	Weekly
Normal	1 Business Day	Quarterly Review for All Open Issues	None	None
Low	2 Business Days	Semi-Annual Review for All Open Issues	None	None

Maintenance and Support Policy: The Maintenance and Support policy is as follows:

AppDynamics provides Maintenance and Support for each version of the Software for a period of twelve (12) months after the generally available release of the next major version of the Software (a major release is a change in the first number to the right of the decimal point). For example, if version 4.1 is released on January 1, 2015, then AppDynamics will provide Maintenance and Support for version 4.0 until January 1, 2016. AppDynamics does not provide Maintenance or Support for any customized software (or components thereof).

For third party software or technology used by End User with the Software but not included with the Software (a "Platform", such as Java Virtual Machines), AppDynamics will follow the end-of-life ("EOL") support timeline announced by the third party vendor of such Platform. AppDynamics will stop providing Maintenance and Support for an EOL'd Platform version when the Platform vendor stops providing maintenance and support for that Platform version.

EXHIBIT B
AVAILABILITY

The terms set forth in this Exhibit B apply only if End User has purchased access to the online software-as-a-service ("SaaS") version of the Software, as indicated on the Order Form.

AVAILABILITY.

AppDynamics will provide Availability (as defined below) for the Software of ninety-nine and one-half percent (99.5%) (the "Availability SLA"), excluding situations identified as "Exclusions" below. For purposes of the Availability SLA, the AppDynamics network extends to, includes and terminates at the data center located router that provides the outside interface of each of AppDynamics' WAN connections to its backbone providers (the "AppDynamics Network"). A report on the actual Availability of the Software is located at https://portal.appdynamics.com/status/saas. The "Controller" is the central repository and analytics engine where all performance data is stored, baselined, and analyzed.

"Exclusions" means any outage that results from any of the following:

a. Any Maintenance performed by AppDynamics during AppDynamics' standard Maintenance windows. AppDynamics will notify End User within forty-eight (48) hours of any standard Maintenance and within twenty-four (24) hours for other non-standard emergency Maintenance (collectively referred to herein as "Scheduled Maintenance").
b. End User's information content or application programming, or the acts or omissions of End User or its agents, including, without limitation, the following:
    1. End User's use of any programs not supplied by AppDynamics;
    2. End User's failure to provide AppDynamics with reasonable advance prior notice of any pending unusual large deployments of new nodes (i.e., adding over ten percent (10%) total nodes in less than twenty-four (24) hours);
    3. End User's implementation of any significant configuration changes, including changes that lead to a greater than thirty percent (30%) change in a one week period or greater than fifty percent (50%) change in a one month period in the number of key objects in the system including but not limited to metrics, snapshots, nodes, events and business transactions;
    4. Any misconfiguration by End User (as determined in AppDynamics' sole discretion), including configuration errors or unintended usage of the Software;
    5. End User's failure to upgrade the Agents to keep the Agent versions within six (6) months of the Controller version; or
    6. End User's implementation of configuration changes in the number of key objects in the Software (including metrics, snapshots, nodes, events and business transactions) that results in, or is likely to result in, an adverse impact on other customers;
c. Force majeure or other circumstances beyond AppDynamics' reasonable control that could not be avoided by its exercise of due care.
d. Failures of the Internet backbone itself and the network by which End User connects to the Internet backbone or any other network unavailability outside of the AppDynamics Network, such as misconfigurations, proxies or firewalls.
e. Any window of time when End User agrees that Software availability/unavailability will not be monitored or counted.
f. Any problems resulting from End User combining or merging the Software with any hardware or software not supplied by AppDynamics or not identified by AppDynamics in the Documentation as being compatible with the Software.
g. End User's or any third party's use of the Software in an unauthorized or unlawful manner.

Remedies for Excessive Downtime:

In the event the Availability of the Software falls below the Availability SLA in a given calendar quarter, AppDynamics will pay End User a service credit ("Service Credit") as follows, corresponding to the actual Availability of the Software during the applicable calendar quarter (on pro-rated basis): if the Availability is 99.5% or greater, End User is entitled to receive no credits; if the Availability is 97.0% - 99.49%, then End User is entitled to receive Service Credits equal to five percent of the fees for the applicable calendar quarter; if the Availability is 95.0% - 96.9%, then End User is entitled to receive Service Credits equal to ten percent of the fees for the applicable calendar quarter; and if the Availability is less than 95.0%, then End User is entitled to receive Service Credits equal to twenty percent of the fees for the applicable calendar quarter. Such Service Credit will be issued as a credit against any fees owed by End User for the next calendar quarter of the Term, or, if End User does not owe any additional fees, then AppDynamics will pay End User the amount of the applicable Service Credit within thirty (30) days after the end of the calendar quarter in which such credit accrued. To receive Service Credits, End User must submit a written request to AppDynamics (to legal@appdynamics.com) within 15 days after the end of the quarter in which the Software was unavailable, or End User's right to receive Service Credits with respect to such unavailability will be

waived. The remedies stated in this section are End User's sole and exclusive remedies and AppDynamics' sole and exclusive obligations for service interruption or unavailability.

"Availability" is measured by the following formula: (n - y) *100 / n

(1) "n" is the total number of minutes in the given calendar quarter minus the Exclusions (as defined above); and "y" is the total number of minutes in the given calendar quarter that the Controller is not accessible by End User (as determined by AppDynamics' tools).

(2) Specifically excluded from "n and "y" in this calculation are the Exclusions.

Annex B

Data Processing Exhibit

This Exhibit shall apply to the 'processing' of any 'personal data' (each as defined below) by AppDynamics in the course of providing the SaaS (as defined below) version of the Software and/or support to the End User.

1. Data Protection

1.1. The terms of this Exhibit apply only if:

(a) End User is subject to Data Protection Law (as defined below); and

(b) End User collects personal data (as defined below) using the Software, which is stored by AppDynamics.

1.2. *Definitions:* In this Exhibit, the following terms shall have the following meanings:

"controller", **"processor"**, **"data subject"**, **"personal data"** and **"processing"** (and **"process"**) shall have the meanings given in the Data Protection Law;

"Data Protection Law" shall mean Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); and

"**Standard Contractual Clauses**" shall mean the terms at https://trust.appdynamics.com/privacy/dataprotectionclauses which form part of this Exhibit pursuant the European Commission Decision C(2010)593 of 5 February 2010.

1.3. *Relationship of the parties:* End User (the controller) appoints AppDynamics as a processor to process the personal data described in Annex A (the "**Data**"). Each party shall comply with the obligations that apply to it under Data Protection Law.

1.4. *Purpose limitation:* AppDynamics shall process the Data as a processor as necessary to perform its obligations under this Agreement and strictly in accordance with the documented instructions of the End User (the "**Permitted Purpose**"), except where otherwise required by any law.

1.5. *International transfers:* AppDynamics shall not transfer the Data (nor permit the Data to be transferred) outside of the European Economic Area ("**EEA**") unless (i) it has first obtained the End User's prior written consent; and (ii) it takes measures to ensure the transfer is in compliance with Data Protection Law. By agreeing to purchase the software-as-a-service version of the Software as indicated in the Order Form, End User acknowledges and agrees that any personal data it collects using the Software may be transferred outside of the EEA. The Standard Contractual Clauses will apply only to personal data that is transferred outside the EEA, either directly or via onward transfer, to any country not recognised by the European Commission as providing an adequate level of protection for personal data (as described in the Data Protection Laws). The Standard Contractual Clauses will not apply if AppDynamics has adopted Binding Corporate Rules or an alternative recognised compliance standard for the lawful transfer of personal data (as defined in the Data Protection Laws) outside the EEA.

1.6. *Confidentiality of processing:* AppDynamics shall ensure that any person that it authorises to process the Data (including AppDynamics' staff, agents and subcontractors) (an "**Authorised Person**") shall be subject to a duty of confidentiality (whether a contractual duty or a statutory duty).

1.7. *Security:* The processor shall implement appropriate controls, including technical, organisational, and other measures, designed to protect the Data (i) from accidental or unlawful destruction, and (ii) loss, alteration, unauthorised disclosure of, or access to the Data (a "**Security Incident**").

1.8. *Subcontracting:* AppDynamics shall not subcontract any processing of the Data to a third-party subcontractor without the prior written consent of the End User. Notwithstanding this, the End User consents to AppDynamics engaging

third-party subcontractors to process the Data provided that: (i) AppDynamics provides at least 7 days' notice prior to the addition or removal of any subcontractor (including details of the processing it performs or will perform), which may be given by posting details of such addition or removal at the following URL: https://trust.appdynamics.com/privacy/subprocessors; (ii) AppDynamics imposes data protection terms on any subcontractor it appoints that protect the Data to the same standard provided for by this Clause; and (iii) AppDynamics remains fully liable for any breach of this Clause that is caused by its subcontractor. A list of approved subcontractors as at the date of this Agreement is at https://trust.appdynamics.com/privacy/subprocessors. If the End User refuses to consent to AppDynamics' appointment of a third-party subcontractor on reasonable grounds relating to the protection of the Data, then End User may terminate this Agreement by giving no less than 30 days' written notice.

1.9. *Data subjects' rights:* AppDynamics shall provide reasonable assistance to the End User (at the End User's expense) to enable the End User to respond to any request from a data subject to exercise any of its rights under Data Protection Law (including its rights of access, correction, objection, erasure and data portability, as applicable).

1.10. *Data Protection Impact Assessment:* If the End User reasonably believes that AppDynamics' processing of the Data will result in a high risk to the data protection rights and freedoms of data subjects, it shall promptly inform AppDynamics and AppDynamics shall, if requested by the End User, provide the End User with reasonable information to enable the End User to conduct a data protection impact assessment (taking into account the nature of the processing and the information available to AppDynamics).

1.11. *Security incidents:* Upon becoming aware of a confirmed Security Incident, AppDynamics shall inform the End User without undue delay and shall provide all such timely information and cooperation as the End User may reasonably require in order for the End User to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Data Protection Law. AppDynamics shall further take such measures and actions as it considers necessary to remedy or mitigate the effects of the Security Incident and shall keep the End User informed in connection with the Security Incident.

1.12. *Deletion of Data:* Upon termination or expiry of this Agreement the End User shall send AppDynamics the details of the relevant Data it wishes to be deleted. AppDynamics will effectively destroy all relevant Data along with any medium or document containing said Data within 14 days from receiving the End User's request if the End User has purchased a dedicated AppDynamics instance or within 365 days if the End User is on a shared instance. AppDynamics shall send the End User written confirmation thereof on written request.

1.13. *End User Audit:* AppDynamics engages a qualified and independent third-party auditor to conduct semi-annual SOC 2 Type II audits in order to evaluate the adequacy of AppDynamics' information security program. Each such audit results in the generation of an audit report ("**Report**"), which shall be AppDynamics' Confidential Information. During the Licence Term, AppDynamics shall: (i) maintain SOC 2 Type II certification (or other industry-recognized successor certification); (ii) at End User's written request, not more than once per calendar year, provide End User with the then-current Report; and (iii) at End User's expense, promptly (taking into account the nature of the request and to the extent reasonably feasible from a technical perspective) comply with any request of End User for information (including any books and/or records) relating to the Software and/or Services as necessary for End User to enable it to comply with Data Protection Law or any request from a regulator. End User agrees that any audit and inspection rights it may have under Data Protection Law shall be satisfied by the obligations in this Clause 1.13.

1.14. *Further Security Information:* At End User's expense, AppDynamics shall further provide detailed written responses (on a confidential basis) to all reasonable requests for information made by End User, including responses to information security and audit questionnaires, that are necessary to confirm AppDynamics' compliance with this Agreement.

1.15. *Regulator Audits:* If a regulator wishes to carry out any audit or inspection of AppDynamics or its activities under this Agreement, End User shall provide AppDynamics at least 30 days' advance notice of any audit, except where the

regulator has given less notice to End User or AppDynamics. AppDynamics shall provide access for any audit or investigation by regulator(s) or law enforcement agent(s) as they require.

Annex A to the Data Processing Exhibit

Subject Matter of Processing

The extraction, collection, storage and analysis of Data generated by, and through, the use of End User's software applications.

Further information about what processing of Data each Software product can be used for can be found at www.appdynamics.com/product and in the Documentation.

Duration of Processing

For the Licence Term of the SaaS Software licence.

Nature and Purpose of Processing

The Data will be processed by AppDynamics SaaS Software platform in order to improve the efficiency and functioning of monitored website(s), software and/or server(s) of End User.

The Software enables the End User to:

- Measure and track response time, load, error rate, slow rate, and stalls for application transactions.
- Auto-discover and map application tiers and services, and see the relationships between them.
- Learn "normal" performance behaviour and "normal" code execution paths for application transactions and application services over time so that anomalies can be detected automatically.
- Follow the flow of application transactions across tiers and services (even in a highly distributed environment) to allow the identification of bottlenecks.
- Identify the root cause of errors in applications.
- View reports and obtain visibility into application performance for understanding the service levels of such applications.
- View operational dashboards to help information technology teams understand the health and performance of application environments.
- View agile release comparisons so that developers understand the business impact of application releases, for the purpose of identifying regression and learning from production deployments.

In the course of monitoring End User's website(s), software and/or server(s), AppDynamics will necessarily ingest and process the Data described above in this Annex A for the purpose of providing the Software and its functions.

Type of Personal Data and Categories of Personal Data

Depending on the End User's configuration of the Software the following types and categories of personal data that might be collected are:

Personal details
Included in this category are classes of data which identify the data subject and their personal characteristics. Examples are names, addresses, job title, employer, contact details, age, sex, date of birth, physical descriptions, identifiers issued by public bodies, e.g. NI number.

Family, lifestyle and social circumstances
Included in this category are any matters relating to the family of the data subject and the data subject's lifestyle and social circumstances. Examples are details about current marriage and partnerships and marital history, details of family and other household members, habits, housing, travel details, leisure activities, membership of charitable or voluntary organisations.

Education and training details
Included in this category are any matters which relate to the education and any professional training of the data subject. Examples are academic records, qualifications, skills, training records, professional expertise, student and pupil records.

Employment details
Included in this category are any matters relating to the employment of the data subject. Examples are employment and career history, recruitment and termination details, attendance record, health and safety records, performance appraisals, training records, security records.

Financial details
Included in this category are any matters relating to the financial affairs of the data subject. Examples are income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, pension information.

Goods or services provided
Included in this category are classes of data relating to goods and services which have been provided. Examples are details of the goods or services supplied, licences issued, agreements and contracts.

IT information
Included in this category is any information relating to an individual's use of technology or software including IP addresses, any information about the computing or mobile device a person is using, location data gathered from such devices, usernames and passwords, social media handles.

Categories of Data Subjects

Customers and/or employees of End User depending on whether End User uses the Software to monitor customer and/or employee facing software applications.

22. APPENDIX: AMAZON CLOUDFRONT SLA (AS OF 6-29-2018)

CloudFront SLA

PRODUCTS & SERVICES

- Amazon CloudFront
- CloudFront SLA
- Streaming
- What's New?
- Dynamic Content Delivery
- Reports & Analytics
- Amazon CloudFront Partners

RELATED LINKS

- Documentation
- AWS Management Console
- Release Notes
- Discussion Forums

Amazon CloudFront Service Level Agreement

Last Updated June 1, 2013

This Amazon CloudFront Service Level Agreement ("SLA") is a policy governing the use of Amazon CloudFront under the terms of the Amazon Web Services Customer Agreement (the "AWS Agreement") between Amazon Web Services, Inc. and its affiliates ("AWS", "us" or "we") and users of AWS' services ("you"). This SLA applies separately to each account using Amazon CloudFront. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement

Service Commitment

AWS will use commercially reasonable efforts to make Amazon CloudFront available with a Monthly Uptime Percentage (defined below) of at least 99.9% during any monthly billing cycle (the "Service Commitment"). In the event Amazon CloudFront does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- "Error Rate" means: (i) the total number of internal server errors returned by Amazon CloudFront divided by (ii) the total number of requests during that five minute period. We will calculate the Error Rate for each Amazon CloudFront account as a percentage for each five minute period in the monthly billing cycle. The calculation of the number of internal server errors will not include errors that arise directly or indirectly as a result of any of the Amazon CloudFront SLA Exclusions (as defined below).
- "Monthly Uptime Percentage" is calculated by subtracting from 100% the average of the Error Rates from each five minute period in the monthly billing cycle.
- A "Service Credit" is a dollar credit, calculated as set forth below, that we may credit back to an eligible account.

https://aws.amazon.com/cloudfront/sla/[6/29/2018 2:30:26 PM]

CloudFront SLA

Service Credits

Service Credits are calculated as a percentage of the total charges paid by you for Amazon CloudFront for the billing cycle in which the error occurred in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Equal to or greater than 99% but less than 99.9%	10%
less than 99%	25%

We will apply any Service Credits only against future Amazon CloudFront payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the error occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide Amazon CloudFront is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

i. the words "SLA Credit Request" in the subject line;

ii. the dates and times of each incident of non-zero Error Rates that you are claiming; and

iii. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage applicable to the month of such request is confirmed by us and is less than 99.9%, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

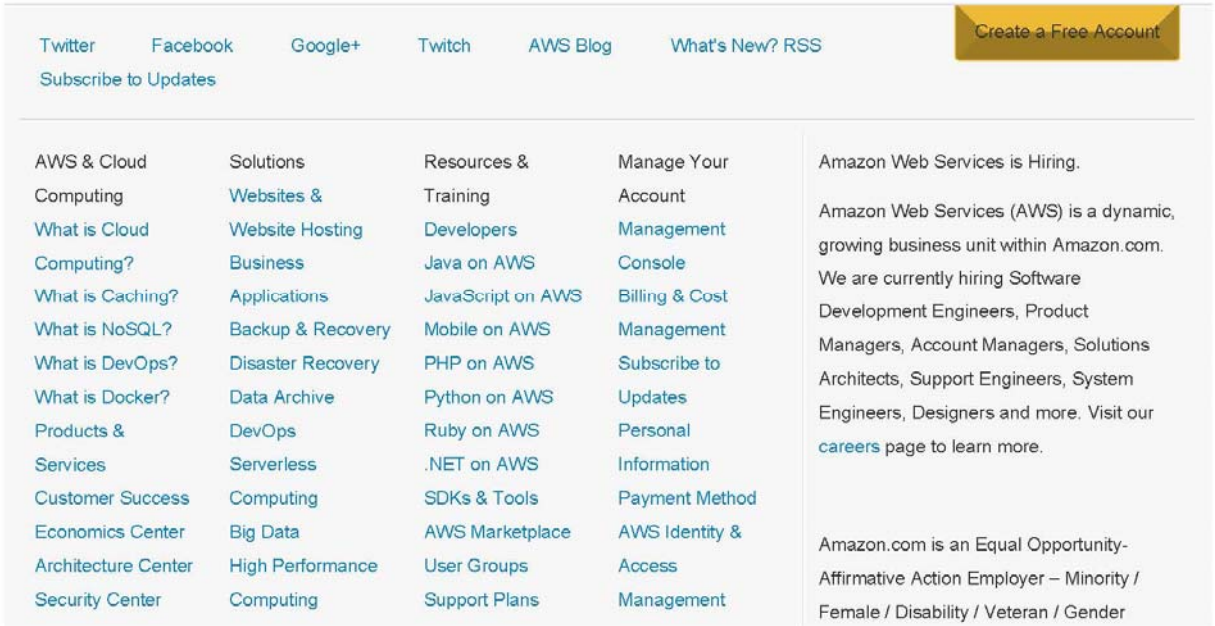
https://aws.amazon.com/cloudfront/sla/[6/29/2018 2:30:26 PM]

CloudFront SLA

Amazon CloudFront SLA Exclusions

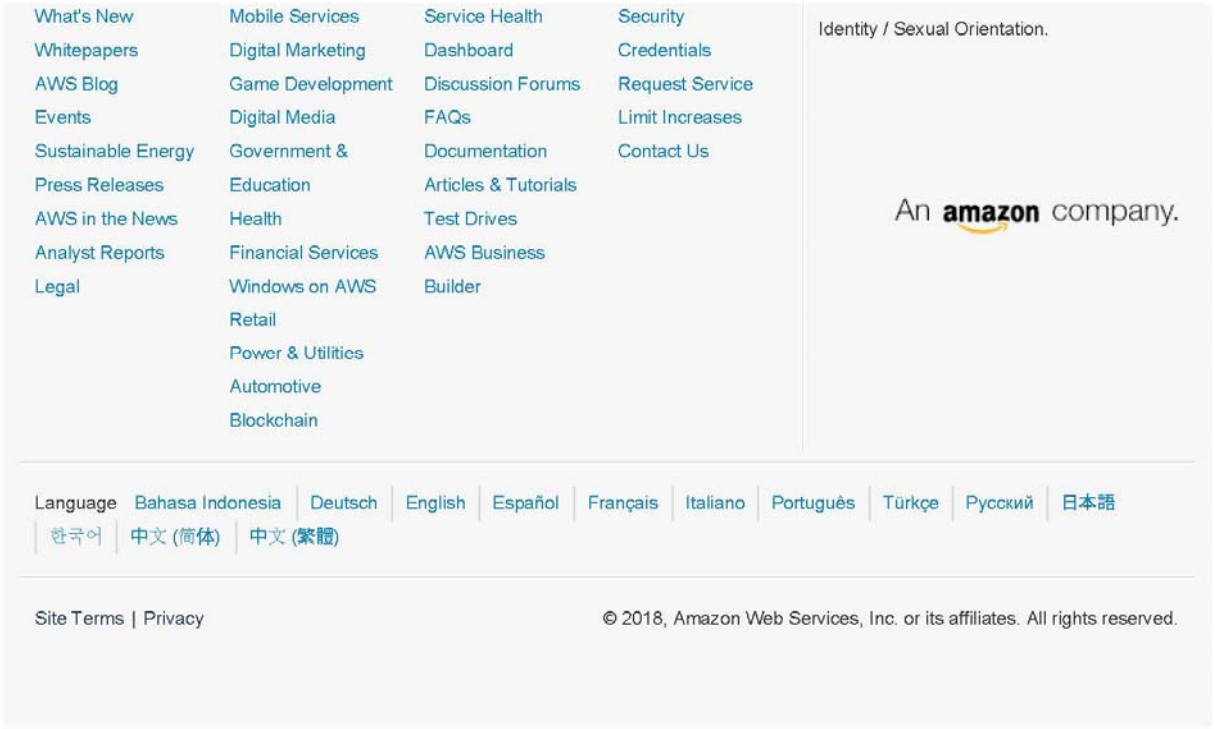
The Service Commitment does not apply to any unavailability, suspension or termination of Amazon CloudFront, or any other Amazon CloudFront performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon CloudFront; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) arising from our suspension and termination of your right to use Amazon CloudFront in accordance with the AWS Agreement; (vi) that result from exceeding usage limits stated in the Amazon CloudFront documentation; or (vii) that result from use of an origin server other than Amazon S3 (collectively, the "Amazon CloudFront SLA Exclusions"). If availability is impacted by factors other than those used in our calculation of the Error Rate, then we may issue a Service Credit considering such factors at our discretion.

Prior Version(s)



https://aws.amazon.com/cloudfront/sla/[6/29/2018 2:30:26 PM]

CloudFront SLA



https://aws.amazon.com/cloudfront/sla/[6/29/2018 2:30:26 PM]

23. APPENDIX: AMAZON EC2 SLA (AS OF 6-29-2018)

Amazon Compute Service Level Agreement

Menu English My Account Sign Up

Amazon Compute Service Level Agreement

Last Updated February 12, 2018

This Amazon Compute Service Level Agreement (this "SLA") is a policy governing the use of the Included Products and Services (listed below) by you or the entity you represent ("you") under the terms of the AWS Customer Agreement (the "AWS Agreement") between Amazon Web Services, Inc. and its affiliates ("AWS", "us" or "we") and you. This SLA applies separately to each account using the Included Products and Services. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Included Products and Services

- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Block Store (Amazon EBS)
- Amazon Elastic Container Service (Amazon ECS)
- Amazon Fargate for Amazon ECS (Amazon Fargate)

Service Commitment

AWS will use commercially reasonable efforts to make the Included Products and Services each available with a Monthly Uptime Percentage (defined below) of at least 99.99%, in each case during any monthly billing cycle (the "Service Commitment"). In the event any of the Included Products and Services do not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- "Monthly Uptime Percentage" is calculated by subtracting from 100% the percentage of minutes during the month in which any of the Included Products and Services, as applicable, was in the state of "Region Unavailable." Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Amazon Compute Services SLA Exclusion (defined below).

https://aws.amazon.com/compute/sla/[6/29/2018 2:31:29 PM]

- "Availability Zone" and "AZ" mean an isolated location within a region identified by a letter identifier following the region code (e.g., us-west-1a).
- "Region Unavailable" and "Region Unavailability" mean:
  - For Regions with only one AZ, when that AZ and one AZ in any other Region, in which you are running an instance or task (one or more containers), as applicable, are concurrently "Unavailable" to you.
  - For all other Regions, when more than one AZ within the same Region, in which you are running an instance or task (one or more containers), as applicable, are concurrently "Unavailable" to you.
- "Unavailable" and "Unavailability" mean:
  - For Amazon EC2, Amazon ECS, or Amazon Fargate, when all of your running instances or running tasks, as applicable, have no external connectivity.
  - For Amazon EBS, when all of your attached volumes perform zero read write IO, with pending IO in the queue.
- A "Service Credit" is a dollar credit, calculated as set forth below, that we may credit back to an eligible account.

Service Commitments and Service Credits

Service Credits are calculated as a percentage of the total charges paid by you (excluding one-time payments such as upfront payments made for Reserved Instances) for either Amazon EC2 or Amazon EBS (whichever was Unavailable, or both if both were Unavailable) in the Region affected for the monthly billing cycle in which the Region Unavailability occurred in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.99% but equal to or greater than 99.0%	10%
Less than 99.0%	30%

We will apply any Service Credits only against future Amazon EC2 or Amazon EBS payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Unavailability occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability, non-

performance, or other failure by us to provide Amazon EC2 or Amazon EBS is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

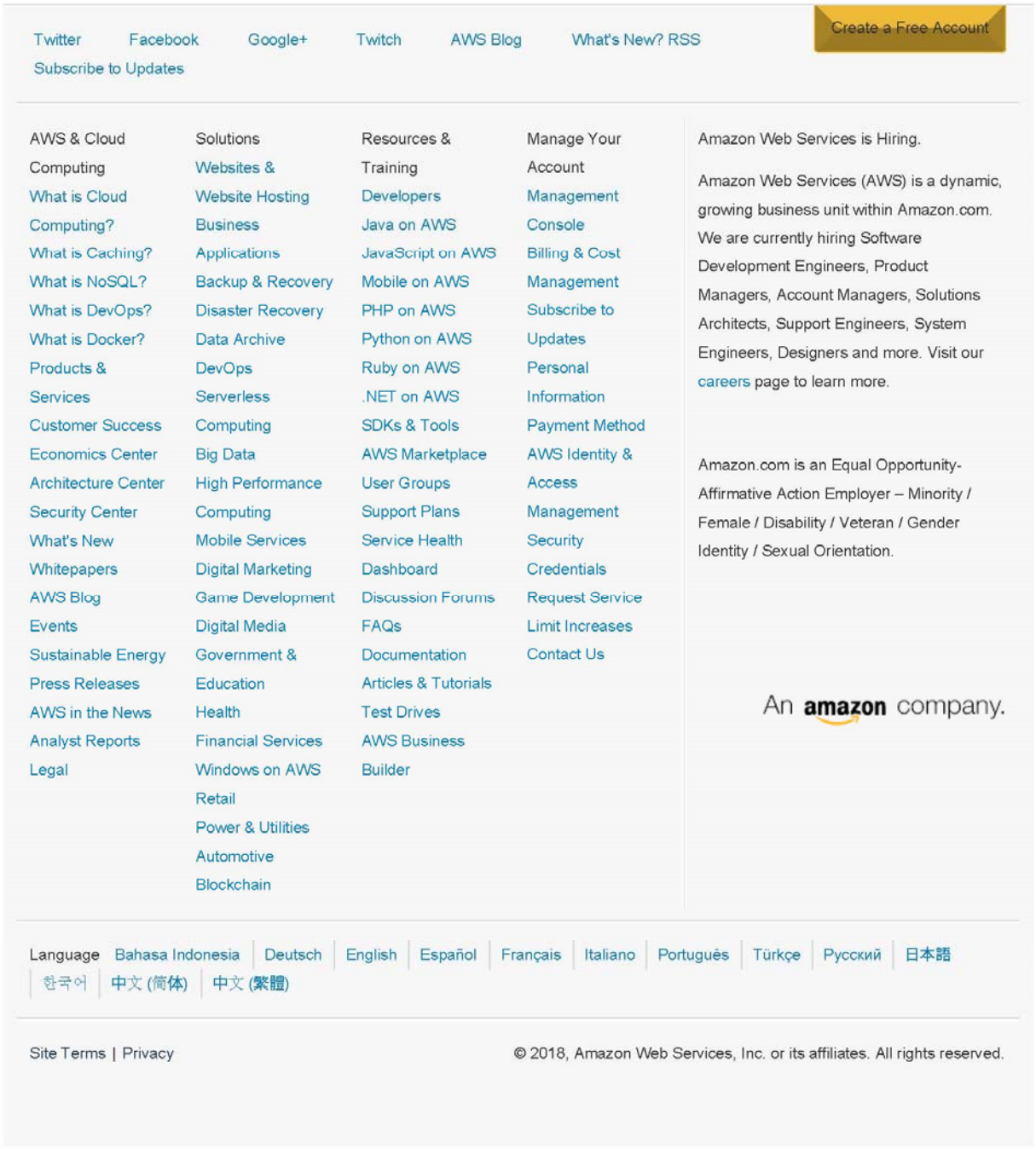
1. the words "SLA Credit Request" in the subject line;
2. the dates and times of each Unavailability incident that you are claiming;
3. the affected EC2 instance IDs or the affected EBS volume IDs; and
4. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage of such request is confirmed by us and is less than the Service Commitment, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon EC2 SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon EC2 or Amazon EBS, or any other Amazon EC2 or Amazon EBS performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon EC2 or Amazon EBS; (iii) that result from any actions or inactions of you or any third party, including failure to acknowledge a recovery volume; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) that result from failures of individual instances or volumes not attributable to Region Unavailability; (vi) that result from any maintenance as provided for pursuant to the AWS Agreement; or (vii) arising from our suspension and termination of your right to use Amazon EC2 or Amazon EBS in accordance with the AWS Agreement (collectively, the "Amazon EC2 SLA Exclusions"). If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.

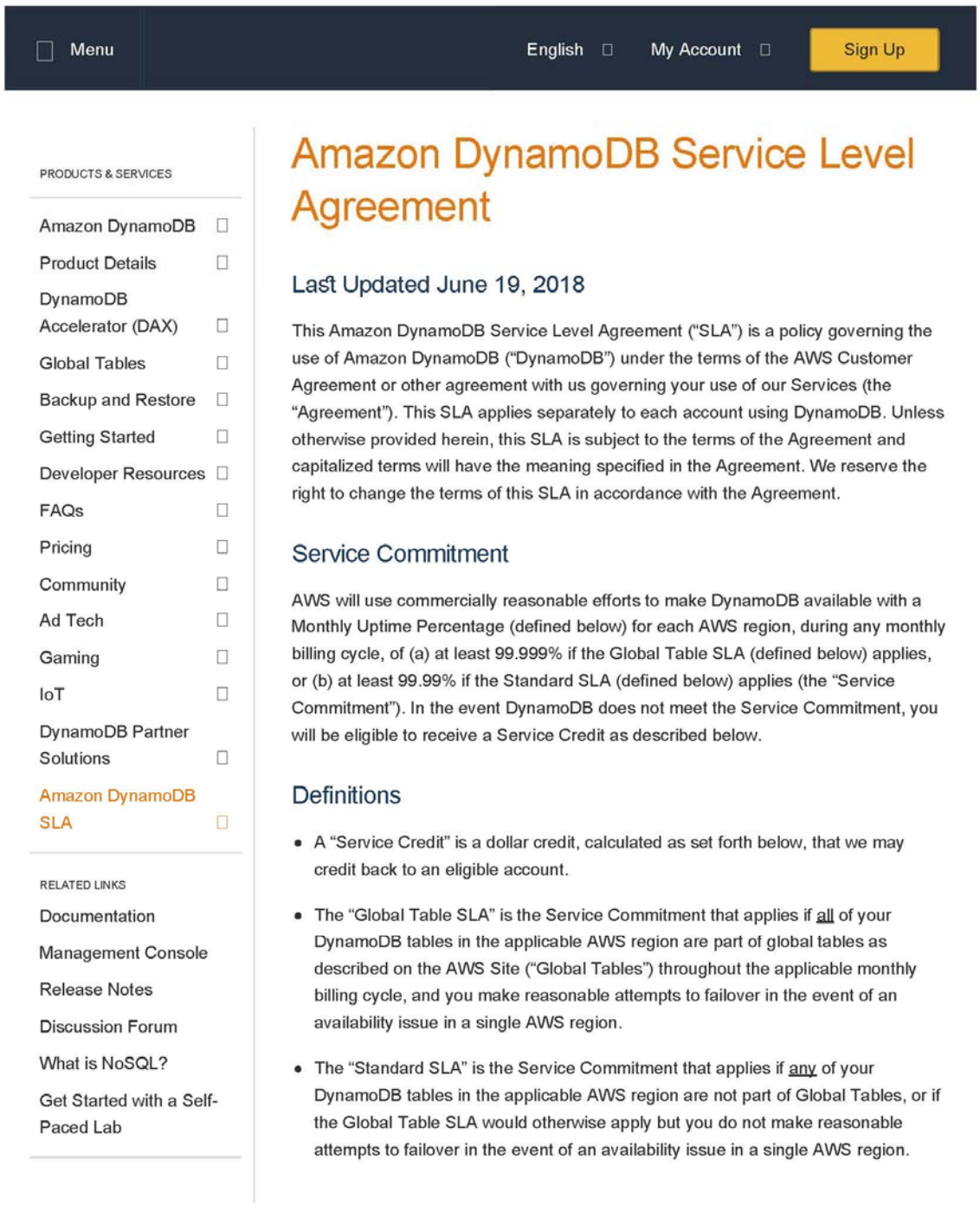
Amazon Compute Service Level Agreement



https://aws.amazon.com/compute/sla/[6/29/2018 2:31:29 PM]

24. APPENDIX: AMAZON DYNAMO DB SLA (AS OF 6-29-2018)

Amazon DynamoDB SLA



https://aws.amazon.com/dynamodb/sla/[6/29/2018 2:30:57 PM]

Amazon DynamoDB SLA

"Monthly Uptime Percentage" for a given AWS region is calculated as the average of the Availability for all 5-minute intervals in a monthly billing cycle. Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any DynamoDB SLA Exclusion (defined below).

- "Availability" is calculated for each 5-minute interval as the percentage of Requests (defined below) processed by DynamoDB that do not fail with Errors (defined below). If you did not make any Requests in a given 5-minute interval, that interval is assumed to be 100% available.
  - The Global Table SLA Availability calculation considers all Requests for all of your DynamoDB tables in the AWS region and also their corresponding replica tables in other AWS regions.
  - The Standard SLA Availability calculation considers all Requests for all of your DynamoDB tables in the applicable AWS region.
- A "Request" is a customer-initiated action of a type specifically listed as being supported by DynamoDB in the DynamoDB API Reference Documentation on the AWS Site. For the avoidance of doubt, Requests do not include actions listed under other products or services (e.g., Amazon DynamoDB Accelerator, Amazon DynamoDB Streams).
- An "Error" is any Request that returns a 500 or 503 error code, as described in DynamoDB Common Errors on the AWS Site.

Service Credits

Service Credits are calculated as a percentage of the following charges paid by you for DynamoDB for the monthly billing cycle in which the Monthly Uptime Percentage for a given AWS region fell within the ranges set forth in the table below: (a) if the Global Table SLA applies, the total charges paid by you for DynamoDB for the AWS region plus the charges described in the "Global Tables" section of the Amazon DynamoDB Pricing page of the AWS Site paid by you for corresponding replica tables in other AWS regions, or (b) if the Standard SLA applies, the total charges paid by you for DynamoDB in the applicable AWS region.

	Monthly Uptime Percentage	Service Credit Percentage
Global Table SLA	Less than 99.999% but equal to or greater than 99%	10%
	Less than 99%	25%
	Less than 99.99% but equal to or greater	10%

https://aws.amazon.com/dynamodb/sla/[6/29/2018 2:30:57 PM]

Standard SLA	than 99%	
	Less than 99%	25%

We will apply any Service Credits only against future DynamoDB payments otherwise due from you. At our discretion, we may issue the Service Credits to the credit card you used to pay for the billing cycle in which the unavailability occurred. Service Credits will not entitle you to any refund or other payment from AWS. Service Credits will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the Agreement, your sole and exclusive remedy for any unavailability or non-performance or other failure by us to provide DynamoDB is the receipt of Service Credits (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive Service Credits, you will need to submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

i. the words "SLA Credit Request" in the subject line;

ii. the billing cycle and AWS regions with respect to which you are claiming Service Credits, together with the Monthly Uptime Percentage for that AWS region for the billing cycle and the specific dates, times, and Availabilities for each 5-minute interval with less than 100% Availability in that AWS region throughout the billing cycle;

iii. your Request logs that document the errors for your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage of such credit request is confirmed by us and is less than the Service Commitment, then we will issue the Service Credits to you within one billing cycle following the month in which the credit request occurred. Your failure to provide the credit request and other information as required above will disqualify you from receiving Service Credits.

DynamoDB SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of DynamoDB, or any other DynamoDB performance issues:

(i) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation

Amazon DynamoDB SLA

point of DynamoDB;

(ii) that result from any voluntary actions or inactions from you or any third party (e.g. scaling of provisioned capacity, misconfiguring security groups, VPC configurations or credential settings, disabling encryption keys or making the encryption keys inaccessible, etc.);

(iii) that result from you not following the best practices described in the DynamoDB User Guide on the AWS Site;

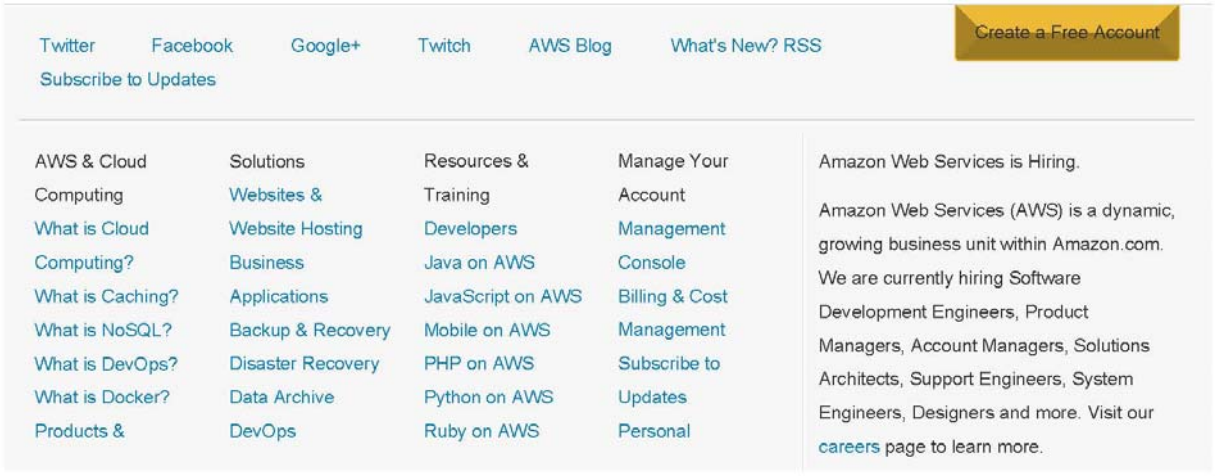
(iv) that result in additional recovery time due to insufficient read capacity units (RCUs) and write capacity units (WCUs) provisioned for your database workload;

(v) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control);

(vi) that result from any maintenance as provided for pursuant to the Agreement; or

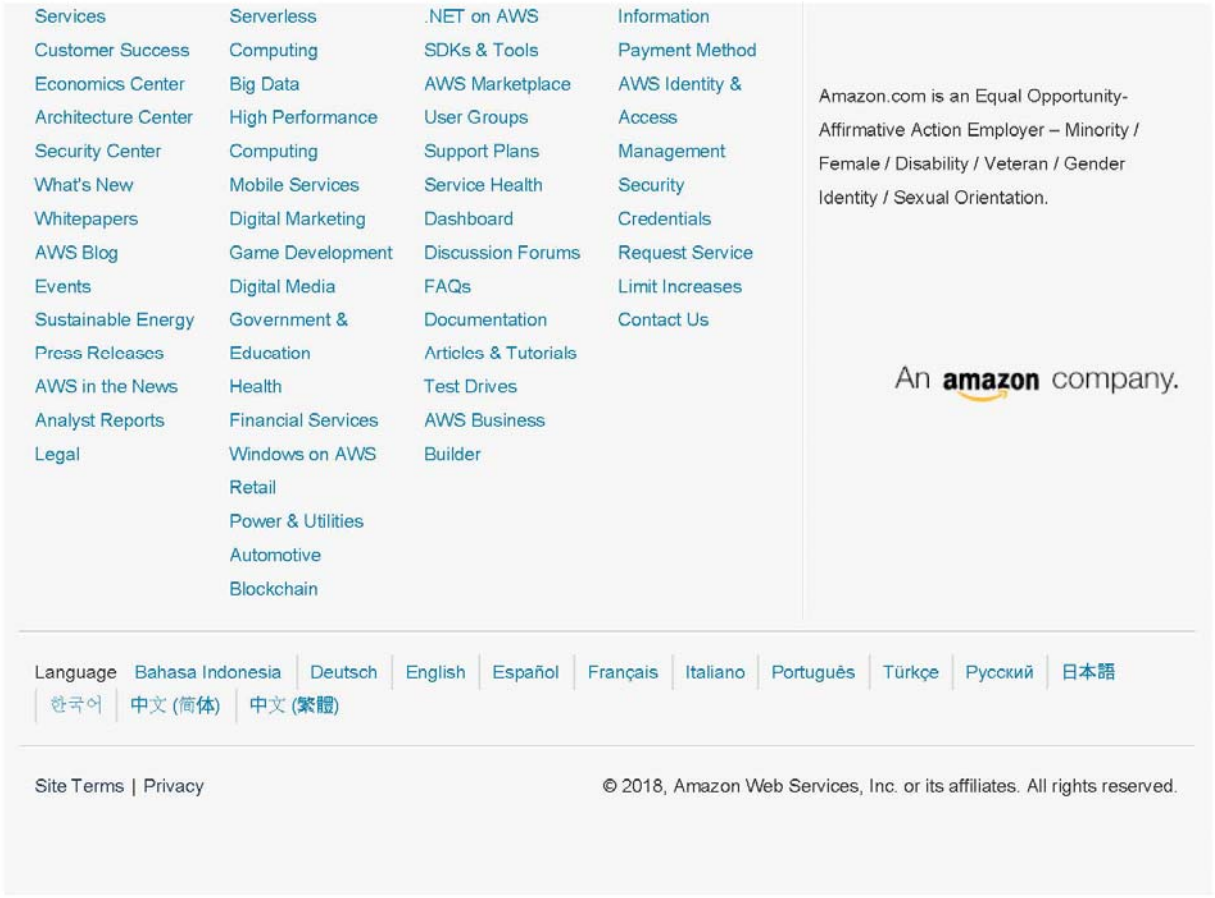
(vii) arising from our suspension and termination of your right to use DynamoDB in accordance with the Agreement (collectively, the "DynamoDB SLA Exclusions").

If availability is impacted by factors other than those explicitly used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.



https://aws.amazon.com/dynamodb/sla/[6/29/2018 2:30:57 PM]

Amazon DynamoDB SLA



https://aws.amazon.com/dynamodb/sla/[6/29/2018 2:30:57 PM]

25. APPENDIX: AMAZON RDS SLA (AS OF 6-29-2018)

Amazon RDS SLA

PRODUCTS & SERVICES

- Amazon RDS
- Product Details
- Instance Types
- Pricing
- FAQs
- Reserved Instances
- Getting Started
- Customer Highlights
- Partners
- Resources
- Amazon RDS SLA

RELATED LINKS

- Amazon Aurora
- Amazon RDS for MySQL
- Amazon RDS for MariaDB
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- Release Notes
- Community Forum
- Documentation

Amazon RDS Service Level Agreement

Create Free Account »

Last Updated March 25, 2016

This Amazon RDS Service Level Agreement ("SLA") is a policy governing the use of the Amazon Relational Database Service ("Amazon RDS") under the terms of the AWS Customer Agreement (the "AWS Agreement") between Amazon Web Services, Inc. and its affiliates ("AWS", "us" or "we") and users of AWS' services ("you"). This SLA applies separately to each account using Amazon RDS. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Multi-AZ instances available with a Monthly Uptime Percentage (defined below) of at least 99.95% during any monthly billing cycle (the "Service Commitment"). In the event Amazon RDS does not meet the Monthly Uptime Percentage commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- "Monthly Uptime Percentage" for a given Multi-AZ instance is calculated by subtracting from 100% the percentage of 1 minute periods during the monthly billing cycle in which the Multi-AZ instance was "Unavailable". If you have been running that Multi-AZ instance for only part of the month, your Multi-AZ instance is assumed to be 100% available for the portion of the month that it was not running. Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Amazon RDS SLA Exclusion (defined below).
- "Multi-AZ instance" means an Amazon RDS for MySQL, MariaDB, Oracle or PostgreSQL database instance with the Multi-AZ parameter set to true.
- "Unavailable" means that all connection requests to the running Multi-AZ instance fail during a 1 minute period.

https://aws.amazon.com/rds/sla/[6/29/2018 2:31:51 PM]

Amazon RDS SLA

- A "Service Credit" is a dollar credit, calculated as set forth below, that we may credit back to an eligible account.

Service Credits

Service Credits are calculated as a percentage of the charges paid by you for the Multi-AZ instances that did not meet the Monthly Uptime Percentage commitment in a billing cycle in accordance with the schedule below.

Monthly Uptime Percentage	Service Credit Percentage
Less than 99.95% but equal to or greater than 99.0%	10%
Less than 99.0%	25%

We will apply any Service Credits only against future Amazon RDS payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the unavailability occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability or non-performance or other failure by us to provide Amazon RDS is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you will need to submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

i. the words "SLA Credit Request" in the subject line;

ii. the dates and times of each Unavailability incident you are claiming;

iii. the DB Instance IDs and the AWS Regions of the affected Multi-AZ instances; and

iv. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage of such request is confirmed by us and is less than the Service Commitment, then we will issue the Service Credit to you within one billing cycle following the month in which the request occurred. Your failure to provide the

https://aws.amazon.com/rds/sla/[6/29/2018 2:31:51 PM]

Amazon RDS SLA

request and other information as required above will disqualify you from receiving a Service Credit.

Amazon RDS SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon RDS, or any other Amazon RDS performance issues:

(i) that result from a suspension described in Section 6.1 of the AWS Agreement;

(ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon RDS;

(iii) that result from any voluntary actions or inactions from you or any third party (e.g., rebooting a database instance, scaling compute capacity, not scaling storage when the storage is full, misconfiguring security groups, VPC configurations or credential settings, disabling encryption keys or making the encryption keys inaccessible, etc.);

(iv) that result from instances belonging to the Micro DB instance class or other instance classes which have similar CPU and memory resource limitations;

(v) that result from you not following the basic operational guidelines described in the Amazon RDS User Guide (e.g., overloading a database instance to the point it is inoperable, creating excessively large number of tables that significantly increase the recovery time etc.);

(vi) caused by underlying database engine software that lead to repeated database crashes or an inoperable database instance;

(vii) that result in long recovery time due to insufficient IO capacity for your database workload;

(viii) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or

(ix) that result from any maintenance as provided for pursuant to the AWS Agreement; or

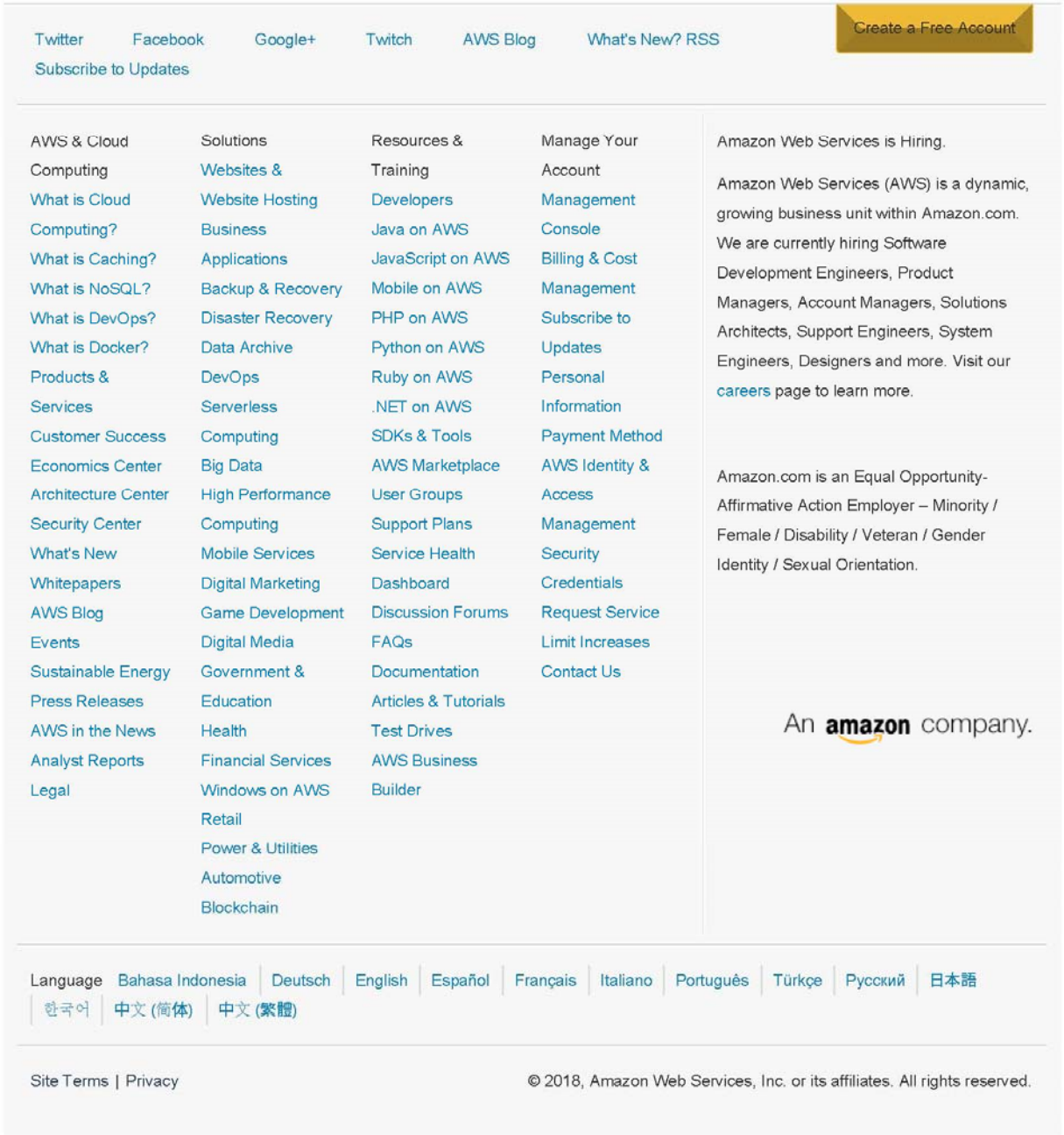
(x) arising from our suspension and termination of your right to use Amazon RDS in accordance with the AWS Agreement (collectively, the "Amazon RDS SLA Exclusions").

If availability is impacted by factors other than those explicitly used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.

Prior Version(s)

https://aws.amazon.com/rds/sla/[6/29/2018 2:31:51 PM]

Amazon RDS SLA



Twitter Facebook Google+ Twitch AWS Blog What's New? RSS
Subscribe to Updates

Create a Free Account

AWS & Cloud Computing
What is Cloud Computing?
What is Caching?
What is NoSQL?
What is DevOps?
What is Docker?
Products & Services
Customer Success
Economics Center
Architecture Center
Security Center
What's New
Whitepapers
AWS Blog
Events
Sustainable Energy
Press Releases
AWS in the News
Analyst Reports
Legal

Solutions
Websites & Website Hosting
Business Applications
Backup & Recovery
Disaster Recovery
Data Archive
DevOps
Serverless Computing
Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services
Windows on AWS
Retail
Power & Utilities
Automotive
Blockchain

Resources & Training
Developers
Java on AWS
JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS
Ruby on AWS
.NET on AWS
SDKs & Tools
AWS Marketplace
User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Test Drives
AWS Business Builder

Manage Your Account
Management Console
Billing & Cost Management
Subscribe to Updates
Personal Information
Payment Method
AWS Identity & Access Management
Security Credentials
Request Service
Limit Increases
Contact Us

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our careers page to learn more.

Amazon.com is an Equal Opportunity-Affirmative Action Employer – Minority / Female / Disability / Veteran / Gender Identity / Sexual Orientation.

An amazon company.

Language Bahasa Indonesia | Deutsch | English | Español | Français | Italiano | Português | Türkçe | Русский | 日本語 | 한국어 | 中文 (简体) | 中文 (繁體)

Site Terms | Privacy

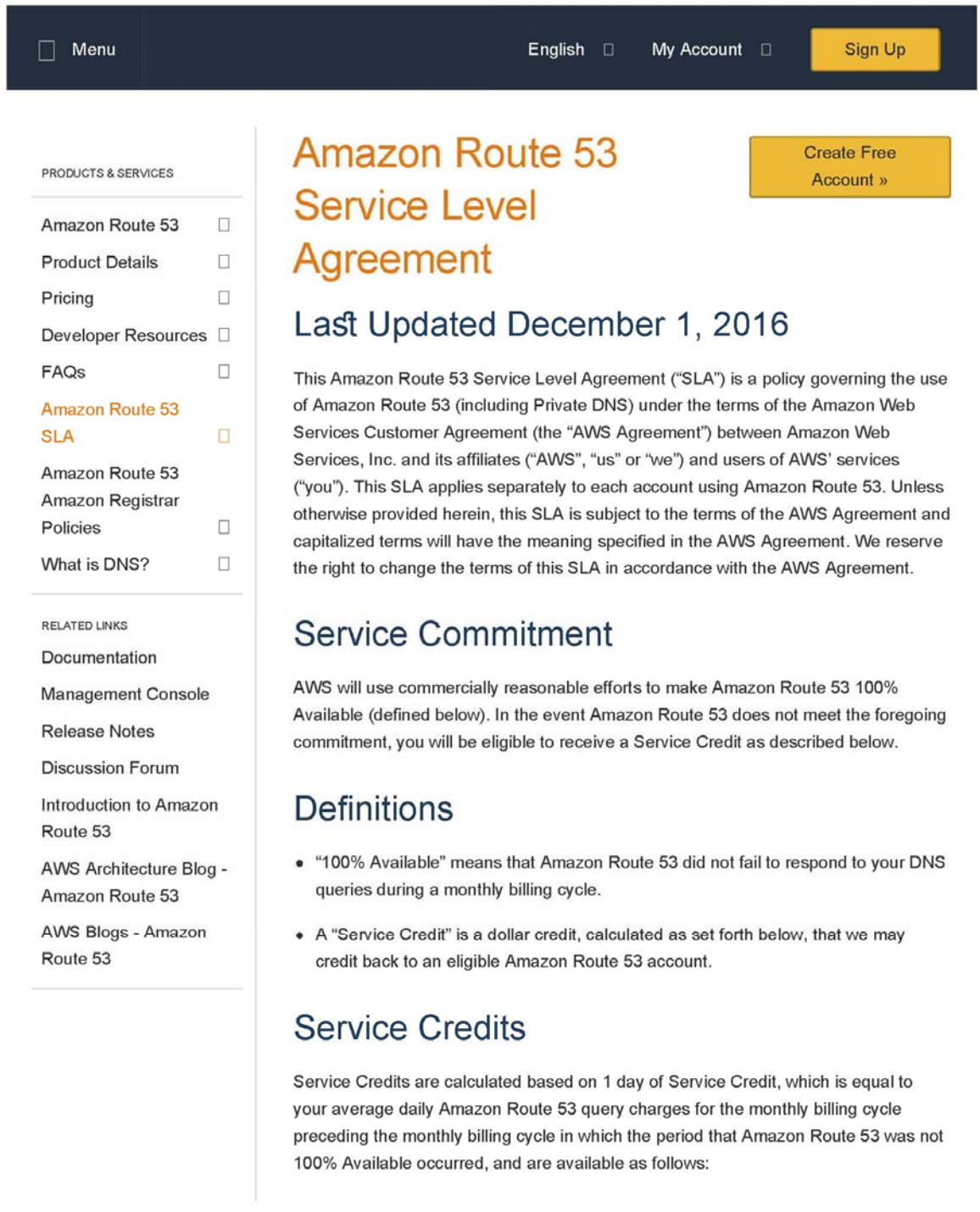
© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

https://aws.amazon.com/rds/sla/[6/29/2018 2:31:51 PM]

Amazon RDS SLA

26. APPENDIX: AMAZON ROUTE 53 SLA (AS OF 6-29-2018)

Amazon Route 53 SLA



https://aws.amazon.com/route53/sla/[6/29/2018 2:32:09 PM]

Amazon Route 53 SLA

Duration Amazon Route 53 was not 100% Available	Service Credit
5 - 30 minutes	1 day Service Credit
31 minutes - 4 hours	7 days Service Credit
More than 4 hours	30 days Service Credit

We will apply any Service Credits only against future Amazon Route 53 payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the error occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide Amazon Route 53 is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

i. the words "SLA Credit Request" in the subject line;

ii. the dates and times of each period that Amazon Route 53 was not 100% Available that you are claiming; and

iii. your request logs that document the errors and corroborate your claimed outage (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the period that Amazon Route 53 was not 100% Available is confirmed by us, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon Route 53 SLA Exclusions

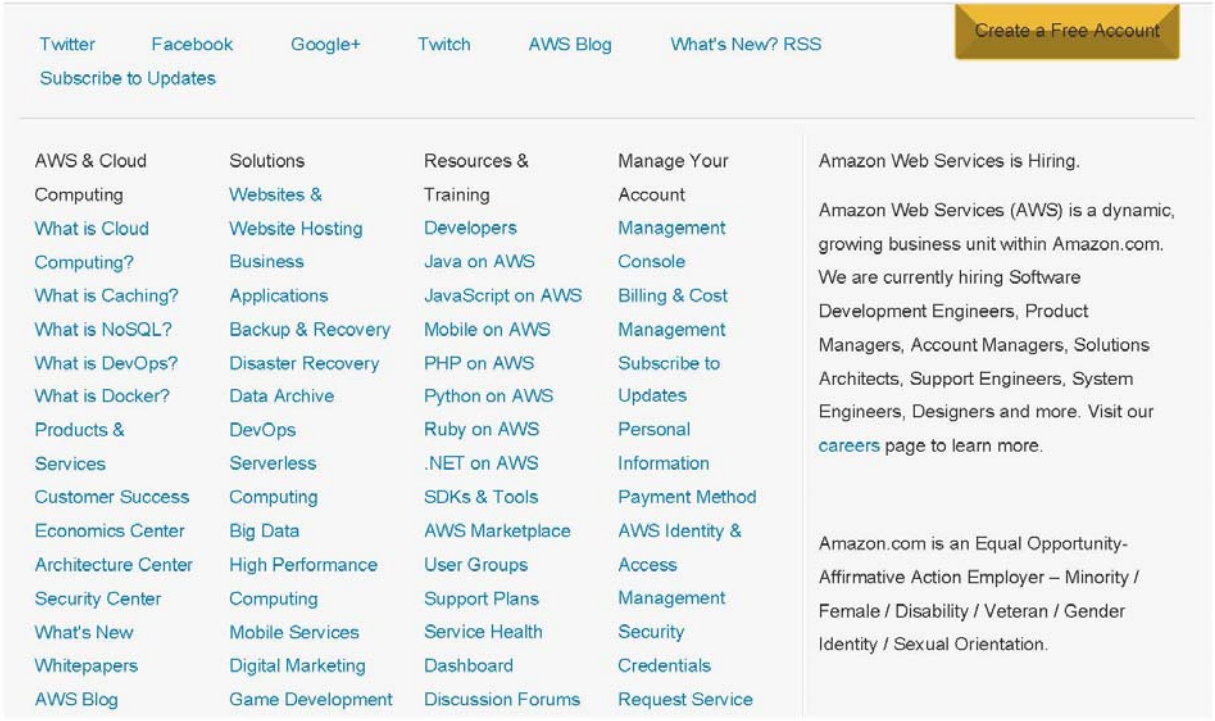
The Service Commitment does not apply to any unavailability, suspension or termination of Amazon Route 53, or any other Amazon Route 53 performance issues:

https://aws.amazon.com/route53/sla/[6/29/2018 2:32:09 PM]

Amazon Route 53 SLA

(i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon Route 53; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) arising from our suspension and termination of your right to use Amazon Route 53 in accordance with the AWS Agreement; (vi) that result from you exceeding usage limits stated in the Amazon Route 53 documentation; or (vii) that, with respect to public DNS only, result during a period that you were not using all four virtual name servers (for example, ns123.awsdns.com, ns123.awsdns.net, ns123.awsdns.co.uk and ns123.awsdns.org) assigned to your "hosted zone" (collectively, the "Amazon Route 53 SLA Exclusions"). If availability is impacted by factors other than those used in our calculation of 100% Available, then we may issue a Service Credit considering such factors at our discretion.

Prior Version(s)



https://aws.amazon.com/route53/sla/[6/29/2018 2:32:09 PM]

Amazon Route 53 SLA

https://aws.amazon.com/route53/sla/[6/29/2018 2:32:09 PM]

27. APPENDIX: AMAZON S3 SLA (AS OF 6-29-2018)

Service Level Agreement – Amazon Simple Storage Service (S3) – AWS

PRODUCTS & SERVICES

- Amazon S3
- Getting Started
- Developer Resources
- Amazon S3 SLA
- Pricing

RELATED LINKS

- AWS Compute Blog
- AWS Lambda Forum

Amazon S3 Service Level Agreement

Create Free Account »

Last Updated April 4, 2018

This Amazon S3 Service Level Agreement ("SLA") is a policy governing the use of Amazon Simple Storage Service ("Amazon S3") under the terms of the Amazon Web Services Customer Agreement (the "AWS Agreement") between Amazon Web Services, Inc. and its affiliates ("AWS", "us" or "we") and users of AWS' services ("you"). This SLA applies separately to each account using Amazon S3. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Amazon S3 available with the applicable Monthly Uptime Percentage (as defined below) during any monthly billing cycle (the "Service Commitment"). In the event Amazon S3 does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Definitions

- "Error Rate" means: (i) the total number of internal server errors returned by Amazon S3 as error status "InternalError" or "ServiceUnavailable" divided by (ii) the total number of requests for the applicable request type during that five minute period. We will calculate the Error Rate for each Amazon S3 account as a percentage for each five minute period in the monthly billing cycle. The calculation of the number of internal server errors will not include errors that arise directly or indirectly as a result of any of the Amazon S3 SLA Exclusions (as defined below).
- "Monthly Uptime Percentage" is calculated by subtracting from 100% the average of the Error Rates from each five minute period in the monthly billing cycle.
- A "Service Credit" is a dollar credit, calculated as set forth below, that we may credit back to an eligible Amazon S3 account.

Service Credits

https://aws.amazon.com/s3/sla/[6/29/2018 2:32:27 PM]

Service Level Agreement – Amazon Simple Storage Service (S3) – AWS

Service Credits are calculated as a percentage of the total charges paid by you for Amazon S3 for the billing cycle in which the error occurred in accordance with the schedule below.

For all requests not otherwise specified below:

Monthly Uptime Percentage	Service Credit Percentage
Equal to or greater than 99.0% but less than 99.9%	10%
Less than 99.0%	25%

For requests to Amazon S3 Standard – Infrequent Access (Standard-IA) and Amazon S3 One Zone – Infrequent Access (OneZone-IA):

Monthly Uptime Percentage	Service Credit Percentage
Equal to or greater than 98.0% but less than 99.0%	10%
Less than 98.0%	25%

We will apply any Service Credits only against future Amazon S3 payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the error occurred. Service Credits will not entitle you to any refund or other payment from AWS. A Service Credit will be applicable and issued only if the credit amount for the applicable monthly billing cycle is greater than one dollar ($1 USD). Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement, your sole and exclusive remedy for any unavailability, non-performance, or other failure by us to provide Amazon S3 is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

1. the words "SLA Credit Request" in the subject line;
2. the dates and times of each incident of non-zero Error Rates that you are claiming; and
3. your request logs that document the errors and corroborate your claimed outage

https://aws.amazon.com/s3/sla/[6/29/2018 2:32:27 PM]

Service Level Agreement – Amazon Simple Storage Service (S3) – AWS

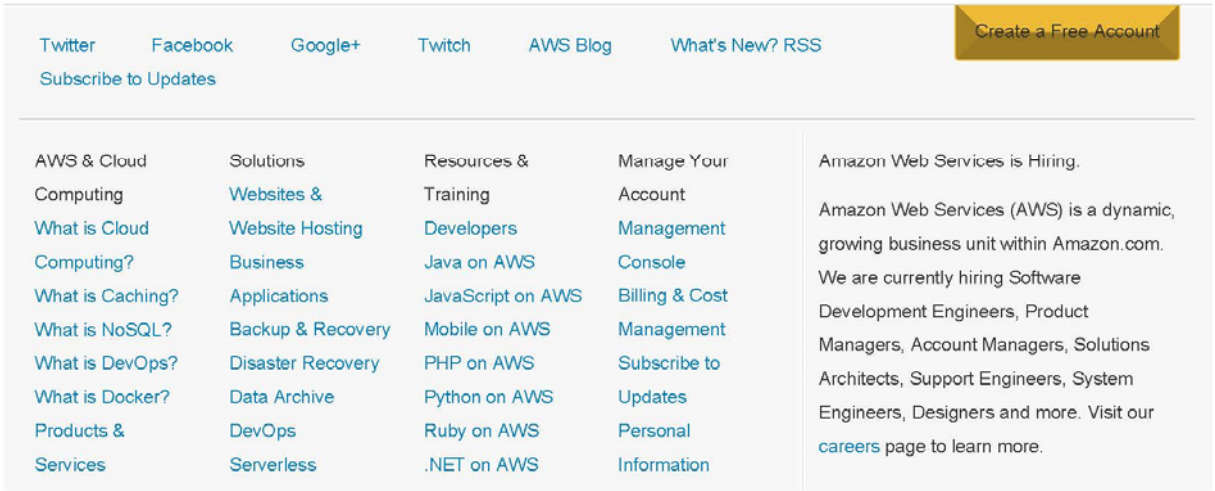
(any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the Monthly Uptime Percentage applicable to the month of such request is confirmed by us and is less than the applicable Service Commitment, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

Amazon S3 SLA Exclusions

The Service Commitment does not apply to any unavailability, suspension or termination of Amazon S3, or any other Amazon S3 performance issues: (i) that result from a suspension described in Section 6.1 of the AWS Agreement; (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Amazon S3; (iii) that result from any actions or inactions of you or any third party; (iv) that result from your equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); or (v) arising from our suspension and termination of your right to use Amazon S3 in accordance with the AWS Agreement (collectively, the "Amazon S3 SLA Exclusions"). If availability is impacted by factors other than those used in our calculation of the Error Rate, then we may issue a Service Credit considering such factors at our discretion.

Prior Version(s)



https://aws.amazon.com/s3/sla/[6/29/2018 2:32:27 PM]

Service Level Agreement – Amazon Simple Storage Service (S3) – AWS

Customer Success
Economics Center
Architecture Center
Security Center
What's New
Whitepapers
AWS Blog
Events
Sustainable Energy
Press Releases
AWS in the News
Analyst Reports
Legal

Computing
Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services
Windows on AWS
Retail
Power & Utilities
Automotive
Blockchain

SDKs & Tools
AWS Marketplace
User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Test Drives
AWS Business Builder

Payment Method
AWS Identity & Access Management
Security Credentials
Request Service Limit Increases
Contact Us

Amazon.com is an Equal Opportunity-Affirmative Action Employer – Minority / Female / Disability / Veteran / Gender Identity / Sexual Orientation.

An amazon company.

Language Bahasa Indonesia | Deutsch | English | Español | Français | Italiano | Português | Türkçe | Русский | 日本語 | 한국어 | 中文 (简体) | 中文 (繁體)

Site Terms | Privacy

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

https://aws.amazon.com/s3/sla/[6/29/2018 2:32:27 PM]

28. APPENDIX: AWS SHIELD ADVANCED SLA (AS OF 6-29-2018)

Service Level Agreement – AWS Shield – AWS

PRODUCTS & SERVICES

- AWS Shield
- Compare Tiers
- Pricing - AWS Shield
- FAQs
- AWS Shield Advanced Service Level Agreement

RELATED LINKS

- AWS Compute Blog
- AWS Lambda Forum

AWS Shield Advanced Service Level Agreement

Create Free Account »

Last Updated December 1, 2016

This AWS Shield Advanced Service Level Agreement ("SLA") is a policy governing your subscription to AWS Shield Advanced under the terms of the Amazon Web Services Customer Agreement (the "AWS Agreement") between Amazon Web Services, Inc. and its affiliates ("AWS", "us" or "we") and users of AWS' services ("you"). This SLA applies separately to each account subscribed to AWS Shield Advanced. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

For Amazon CloudFront and Amazon Route 53 resources designated by you for protection by AWS Shield Advanced, AWS will use commercially reasonable efforts to prevent those resources from failing to meet any service commitments specified in the Amazon CloudFront Service Level Agreement or Route 53 Service Level Agreement as a result of any denial-of-service attack covered by AWS Shield Advanced (the "Service Commitment"). In the event AWS Shield Advanced does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below. For Amazon CloudFront and Amazon Route 53 resources designated by you for protection by AWS Shield Advanced, a denial-of-service attack covered by AWS Shield Advanced will not constitute an Amazon CloudFront SLA Exclusion or Amazon Route 53 SLA Exclusion (as defined in the Amazon CloudFront Service Level Agreement and the Amazon Route 53 Service Level Agreement, respectively) with respect to a failure to meet any service commitments specified in the Amazon CloudFront Service Level Agreement or Route 53 Service Level Agreement.

Service Credits

For each 24-hour period (Coordinated Universal Time) in which Amazon CloudFront or Amazon Route 53 experienced an availability interruption that contributed to AWS

https://aws.amazon.com/shield/sla/[6/29/2018 3:42:55 PM]

Service Level Agreement – AWS Shield – AWS

Shield Advanced not meeting the Service Commitment you are entitled to a "Service Credit" in an amount equal to the average daily charges for AWS Shield Advanced for the monthly billing cycle in which the Service Commitment failure occurred. We will apply any Service Credits only against future AWS Shield Advanced payments otherwise due from you. At our discretion, we may issue the Service Credit to the credit card you used to pay for the billing cycle in which the Service Commitment failure occurred. Service Credits will not entitle you to any refund or other payment from AWS. Service Credits may not be transferred or applied to any other account. Unless otherwise provided in the AWS Agreement (including the Amazon CloudFront Service Level Agreement or Amazon Route 53 Service Level Agreement), your sole and exclusive remedy for any unavailability of the AWS resources designated by you for protection by AWS Shield Advanced is the receipt of a Service Credit (if eligible) in accordance with the terms of this SLA.

Credit Request and Payment Procedures

To receive a Service Credit, you must submit a claim by opening a case in the AWS Support Center. To be eligible, the credit request must be received by us by the end of the second billing cycle after which the incident occurred and must include:

i. the words "SLA Credit Request" in the subject line;

ii. the dates and times of each incident of availability interruption that you are claiming; and

iii. your request logs that document the errors and corroborate your claimed availability interruption (any confidential or sensitive information in these logs should be removed or replaced with asterisks).

If the failure to meet the Service Commitment is confirmed by us, then we will issue the Service Credit to you within one billing cycle following the month in which your request is confirmed by us. Your failure to provide the request and other information as required above will disqualify you from receiving a Service Credit.

https://aws.amazon.com/shield/sla/[6/29/2018 3:42:55 PM]

Service Level Agreement – AWS Shield – AWS

What is Caching?
What is NoSQL?
What is DevOps?
What is Docker?
Products & Services
Customer Success
Economics Center
Architecture Center
Security Center
What's New
Whitepapers
AWS Blog
Events
Sustainable Energy
Press Releases
AWS in the News
Analyst Reports
Legal

Applications
Backup & Recovery
Disaster Recovery
Data Archive
DevOps
Serverless Computing
Big Data
High Performance Computing
Mobile Services
Digital Marketing
Game Development
Digital Media
Government & Education
Health
Financial Services
Windows on AWS
Retail
Power & Utilities
Automotive
Blockchain

JavaScript on AWS
Mobile on AWS
PHP on AWS
Python on AWS
Ruby on AWS
.NET on AWS
SDKs & Tools
AWS Marketplace
User Groups
Support Plans
Service Health Dashboard
Discussion Forums
FAQs
Documentation
Articles & Tutorials
Test Drives
AWS Business Builder

Billing & Cost Management
Subscribe to Updates
Personal Information
Payment Method
AWS Identity & Access Management
Security Credentials
Request Service
Limit Increases
Contact Us

Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our careers page to learn more.

Amazon.com is an Equal Opportunity-Affirmative Action Employer – Minority / Female / Disability / Veteran / Gender Identity / Sexual Orientation.

An amazon company.

Language | Bahasa Indonesia | Deutsch | English | Español | Français | Italiano | Português | Türkçe | Русский | 日本語 | 한국어 | 中文 (简体) | 中文 (繁體)

Site Terms | Privacy

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

https://aws.amazon.com/shield/sla/[6/29/2018 3:42:55 PM]

29. APPENDIX: AWS SERVICE DESCRIPTION

The following Table is provided as a summary of all AWS Services with links to the service website that provide service documentation, pricing information, FAQs, release notes, developer information, and relevant case studies

AWS Service (Hyperlink)	Description
Compute	
Amazon EC2	• Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable computing capacity—literally, servers in Amazon's data centers—that customers use to build and host their software systems. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing customers to quickly scale capacity, both up and down, as their computing requirements change. Amazon EC2 instances in Amazon Virtual Private Cloud (Amazon VPC) offer native support for the IPv6 protocol. • http://aws.amazon.com/documentation/ec2/
Amazon ECS	• Amazon Elastic Container Service (Amazon ECS) is a highly scalable, high performance container management service that supports Docker containers and allows customers to easily run applications on a managed cluster of Amazon EC2 instances. With simple API calls, customers can launch and stop Docker-enabled applications, query the complete state of a cluster, and access many familiar features. Customers can use Amazon ECS to schedule the placement of containers across a cluster based on resource needs and availability requirements. Customers can also integrate their own scheduler or third-party schedulers to meet business or application-specific requirements. Amazon ECS can send container instances and task state changes to CloudWatch Events. • http://aws.amazon.com/ecs/faqs/
Amazon EKS (in Preview)	• Amazon Elastic Container Service for Kubernetes (Amazon EKS) is a managed service that makes it easy for customers to run Kubernetes on AWS without needing to install and operate their own Kubernetes clusters. With Amazon EKS, upgrades and high availability are managed by AWS. Amazon EKS runs three Kubernetes masters across three Availability Zones in order to ensure high availability. Amazon EKS automatically detects and replaces unhealthy masters, and it provides automated version upgrades and patching for the masters.
AWS Fargate	• AWS Fargate is a technology for deploying and managing containers, which frees customers from having to manage any of the underlying infrastructure. With AWS Fargate, customers no longer have to provision, configure, and scale clusters of virtual machines to run containers. Amazon ECS uses containers provisioned by Fargate to automatically scale, load balance, and manage scheduling of containers for availability, providing an easier way to

AWS Service (Hyperlink)	Description
	build and operate containerized applications. AWS Fargate will also support Amazon EKS in 2018.
Amazon ECR	• Amazon Elastic Container Registry (Amazon ECR) is a fully managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images. Amazon ECR is integrated with Amazon ECS, simplifying development-to-production workflows. Amazon ECR eliminates the need for customers to operate their own container repositories or worry about scaling the underlying infrastructure. Amazon ECR hosts images in a highly available and scalable architecture, allowing customers to reliably deploy containers for applications. • https://aws.amazon.com/documentation/ecr/
AWS Elastic Beanstalk	• AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with Java, .NET, PHP, Node.js, Python, Ruby, Go, and Docker on familiar servers such as Apache, Nginx, Passenger, and IIS. Customers can simply upload their code and AWS Elastic Beanstalk automatically handles the deployment, from capacity provisioning, load balancing, and auto scaling to application health monitoring. At the same time, customers retain full control over the AWS resources powering their application and can access the underlying resources at any time. • https://aws.amazon.com/documentation/elastic-beanstalk/
AWS Lambda	• AWS Lambda lets customers run code without provisioning or managing servers. With AWS Lambda, customers can run code for virtually any type of application or back-end service—all with zero administration. Just upload code and AWS Lambda takes care of everything required to run and scale the code with high availability. Customers can set up their code to automatically trigger from other AWS Cloud services or call it directly from any web or mobile application. Customers can also develop their AWS Lambda functions in C# using the .NET Core 1.0 runtime. • http://aws.amazon.com/documentation/lambda/
Auto Scaling	• Auto Scaling is a web service designed to launch or terminate Amazon EC2 instances automatically based on user-defined policies, schedules, and health checks. • http://aws.amazon.com/documentation/autoscaling/
Amazon Lightsail	• Amazon Lightsail is designed to be the easiest way to launch and manage a virtual private server with AWS. Amazon Lightsail plans include everything customer need to jumpstart their project—a virtual machine, SSD-based storage, data transfer, DNS management, and a static IP—for a low, predictable price. Amazon Lightsail virtual private servers run on the same highly available and reliable AWS cloud infrastructure used by millions of customers. • https://amazonlightsail.com/docs/

AWS Service (Hyperlink)	Description
AWS Batch	• AWS Batch is a set of batch management capabilities that enables developers, scientists, and engineers to easily and efficiently run hundreds of thousands of batch computing jobs on AWS. AWS Batch dynamically provisions the optimal quantity and type of compute resources (e.g., CPU or memory optimized instances) based on the volume and specific resource requirements of the batch jobs submitted. With AWS Batch, there is no need to install and manage batch computing software or server clusters, allowing customers to instead focus on analyzing results and solving problems. AWS Batch plans, schedules, and executes batch computing workloads using Amazon EC2 and Spot Instances. • https://aws.amazon.com/batch/faqs/
AWS Serverless Application Repository	• The AWS Serverless Application Repository is a collection of serverless applications and serverless application components provided by AWS and other AWS partners and developers. With a growing selection of applications to choose from, the AWS Serverless Application Repository makes it easy to get started with the AWS serverless platform. The AWS Serverless Application Repository includes applications for Alexa Skills, chatbots, data processing, IoT, real time stream processing, web and mobile back-ends, social media trend analysis, image resizing, and more from publishers on AWS. • http://docs.aws.amazon.com/serverlessrepo/latest/devguide/what-is-serverlessrepo.html
Storage	
Amazon S3	• Amazon Simple Storage Service (Amazon S3) is storage for the Internet. Customers can use Amazon S3 to store and retrieve any amount of data, at any time, from anywhere on the web. Amazon S3 offers a range of storage classes designed for different use cases: Amazon S3 Standard for general-purpose storage of frequently accessed data, Amazon S3 Standard − Infrequent Access (Standard − IA) for long-lived, but less frequently accessed data, and Amazon Glacier for long-term archive. • http://aws.amazon.com/documentation/s3/
Amazon Glacier	• Amazon Glacier is a storage service optimized for infrequently used data, or “cold data.” The service provides secure, durable, and extremely low-cost storage for data archiving and backup. With Amazon Glacier, customers can store their data cost effectively for months, years, or even decades. Amazon Glacier enables customers to offload the administrative burdens of operating and scaling storage to AWS, so customers don't have to worry about capacity planning, hardware provisioning, data replication, hardware failure detection and recovery, or time-consuming hardware migrations. • http://aws.amazon.com/documentation/glacier/
Amazon EBS	• Amazon Elastic Block Store (Amazon EBS) provides block-level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are highly available and reliable storage volumes that can be attached to any

AWS Service (Hyperlink)	Description
	running instance that is in the same Availability Zone. Amazon EBS volumes that are attached to an Amazon EC2 instance are exposed as storage volumes that persist independently from the life of the instance. • http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html
Amazon EFS	• Amazon Elastic File System (Amazon EFS) provides simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud. Amazon EFS is easy to use and offers a simple interface that allows customers to create and configure file systems quickly and easily. With Amazon EFS, storage capacity is elastic, growing and shrinking automatically as files are added and removed, so applications have the storage they need, when they need it. Amazon EFS also allows customers to access file data from on-premises data centers. On-premises servers can move file data to and from an Amazon EFS file systems when connected to an Amazon VPC with AWS Direct Connect, allowing customers to migrate data sets to Amazon EFS, enable cloud bursting scenarios, or back up on-premises data to Amazon EFS. • https://aws.amazon.com/documentation/efs/
AWS Import/Export Disk	• AWS Import/Export Disk accelerates moving large amounts of data into and out of the AWS cloud using portable storage devices for transport. AWS Import/Export Disk transfers data directly onto and off of storage devices using Amazon's high-speed internal network and bypassing the Internet. For significant data sets, AWS Import/Export Disk is often faster than Internet transfer and more cost effective than upgrading connectivity. • http://aws.amazon.com/documentation/importexport/
AWS Storage Gateway	• AWS Storage Gateway is a service that connects an on-premises software appliance with cloud-based storage to provide seamless and secure integration between an on-premises IT environment and AWS's storage infrastructure. AWS Storage Gateway also provides a virtual on-premises file server, which enables customers to store and retrieve Amazon S3 objects through standard file storage protocols. • http://aws.amazon.com/documentation/storagegateway/
Databases	
Amazon RDS	• Amazon Relational Database Service (Amazon RDS) is a web service that makes it easier to set up, operate, and scale a relational database in the cloud. It provides cost-efficient, resizable capacity for an industry-standard relational database and manages common database administration tasks. Database engines available through Amazon RDS include Amazon Aurora, MySQL, Oracle, Microsoft SQL Server 2016, PostgreSQL, and MariaDB. Amazon RDS for Oracle Database Instance supports outbound network access and can send emails using an utl_smtp package, plus communicate with external Web Servers and TCP/IP-based servers using utl_http and utl_tcp packages. • http://aws.amazon.com/documentation/rds/

AWS Service (Hyperlink)	Description
Amazon Aurora	• Amazon Aurora is a MySQL-compatible relational database engine that combines the speed and availability of high-end commercial databases with the simplicity and cost effectiveness of open-source databases. Amazon Aurora provides up to five times better performance than MySQL with the security, availability, and reliability of a commercial database at one-tenth the cost. Amazon Aurora's PostgreSQL support allows customers to get up to several times better performance than the typical PostgreSQL database. • http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_Aurora.html
Amazon DynamoDB	• Amazon DynamoDB is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. Customers can use Amazon DynamoDB to create a database table that can store and retrieve any amount of data and serve any level of request traffic. Amazon DynamoDB automatically spreads the data and traffic for the table over a sufficient number of servers to handle the request capacity specified by the customer and the amount of data stored while maintaining consistent and fast performance. • http://aws.amazon.com/documentation/dynamodb/
Amazon Redshift	• Amazon Redshift is a fast, fully managed, petabyte-scale data warehouse solution that makes it simple and cost effective to efficiently analyze data using your existing business intelligence tools. Customers can start small for just $0.25 per hour with no commitments or upfront costs and scale to a petabyte or more for $1,000 per terabyte per year, less than one-tenth the cost of most other data warehousing solutions. For customer convenience, multibyte (UTF-8) characters can be used in Amazon Redshift table, column, and other database object names. • http://aws.amazon.com/documentation/redshift/
Amazon ElastiCache	• Amazon ElastiCache is a web service that makes it easy to set up, manage, and scale distributed, in-memory cache environments in the cloud. It provides a high-performance, resizable, and cost-effective in-memory cache, while removing the complexity associated with deploying and managing a distributed cache environment. Amazon ElastiCache supports two open-source, in-memory engines: Redis and Memcached. • http://aws.amazon.com/documentation/elasticache/
Migration	
AWS Migration Hub	• AWS Migration Hub provides a single place to discover existing servers and track the status of each application migration. It gives customers better visibility into their application portfolio and streamlines migration tracking. If a customer plans to migrate some or all of their workloads to AWS using tools like AWS Server Migration Service, AWS Database Migration Service, or partner tools, then they should consider using AWS Migration Hub. If a customer is rehosting servers and/or replatforming databases in AWS, then the

AWS Service (Hyperlink)	Description
	AWS Migration Hub can reduce time spent determining current status and next steps. • https://aws.amazon.com/documentation/migrationhub/
AWS Application Discovery Service	• AWS Application Discovery Service helps customers quickly and reliably plan application migration projects by automatically identifying applications running in on-premises data centers, their associated dependencies, and their performance profile. AWS Application Discovery Service automatically collects configuration and usage data from server, storage, and networking equipment to develop a list of applications, how they perform, and how they are interdependent. • https://aws.amazon.com/documentation/application-discovery/
AWS Database Migration Service	• AWS Database Migration Service helps customers migrate databases to AWS easily and securely. The source database remains fully operational during the migration. Customers can migrate data to and from most widely used commercial and open-source databases. The service supports homogenous migrations such as Oracle to Oracle, as well as heterogeneous migrations between different database platforms, such as Oracle to Amazon Aurora or Microsoft SQL Server to MySQL. • https://aws.amazon.com/documentation/dms/
AWS SMS	• AWS Server Migration Service (AWS SMS) is an agentless service which makes it easier and faster for customers to migrate thousands of on-premises workloads to AWS. AWS SMS allows customers to automate, schedule, and track incremental replications of live server volumes, making it easier to coordinate large-scale server migrations. • https://aws.amazon.com/documentation/server-migration-service/
AWS Snowball	• AWS Snowball accelerates transferring large amounts of data between the cloud and portable storage devices that a customer mails to us. AWS transfers data directly onto and off of the customer's storage devices using Amazon's high-speed internal network. The data load typically begins the next business day after the storage device arrives at AWS. After the data export or import completes, we return the storage device. For large data sets, AWS Snowball is significantly faster than Internet transfer and more cost effective than upgrading connectivity. • https://aws.amazon.com/documentation/snowball/
AWS Snowball Edge	• AWS Snowball Edge is a 100TB data transfer device with on-board storage and compute. Customers can use AWS Snowball Edge to move large amounts of data into and out of AWS, as a temporary storage tier for large local data sets, or to support independent local workloads in remote locations. AWS Snowball Edge connects to existing applications and infrastructure using standard storage interfaces. AWS Snowball Edge can cluster together to form a local storage tier and process data on-premises, helping ensure that applications continue to run even when they are not able to access the cloud.

AWS Service (Hyperlink)	Description
	• https://aws.amazon.com/documentation/snowball/
AWS Snowmobile	• AWS Snowmobile is an Exabyte-scale data transfer service that can move extremely large amounts of data to AWS in a fast, secure, and cost-effective manner. Transfer up to 100PB per AWS Snowmobile—a 45-foot long ruggedized shipping container pulled by a semi-trailer truck—to move massive volumes of data to the cloud. All data is encrypted with 256-bit encryption with managed encryption keys using AWS Key Management Service (AWS KMS). AWS Snowmobile includes GPS tracking, alarm monitoring, 24/7 video surveillance and an optional escort security vehicle while in transit. After the data is loaded, AWS Snowmobile is driven back to AWS where the data is imported into Amazon S3 or Amazon Glacier. • https://aws.amazon.com/snowmobile/faqs
Network and Content Delivery	
Amazon VPC	• Amazon Virtual Private Cloud (Amazon VPC) enables customers to launch AWS resources into a virtual network that they've defined. This virtual network closely resembles a traditional network that a customer would operate in their own data center, with the benefits of using the scalable infrastructure of AWS. • http://aws.amazon.com/documentation/vpc/
Amazon CloudFront	• Amazon CloudFront is a content delivery web service. It integrates with other AWS Cloud services to give developers and businesses an easy way to distribute content (for example, streaming video) to end users with low latency, high data transfer speeds, and no commitments. Amazon CloudFront has a type of edge location called Regional Edge Cache that further improves performance for viewers. Regional Edge Caches, in addition to improving performance, help reduce the load on origin resources, minimizing operational burden associated with scaling origin and reducing origin costs. Regional Edge Caches are turned on by default for Amazon CloudFront distributions; customers do not need to make any changes to their distributions to take advantage of this feature. There are also no additional charges to use this feature. • http://aws.amazon.com/documentation/cloudfront/
Amazon Route 53	• Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. It is designed as an extremely reliable and cost-effective way to route users to Internet applications by translating site names into IP addresses. Amazon Route 53 also connects user requests to infrastructure running in AWS, such as Amazon EC2 instances, Elastic Load Balancing load balancers, or Amazon S3 buckets. Amazon Route 53 health checks support endpoints with IPv6 addresses and DNS queries over IPv6. • https://aws.amazon.com/documentation/route53/
Amazon API Gateway	• Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale.

AWS Service (Hyperlink)	Description
	With a few clicks in the AWS Management Console, customers can create an API that acts as a "front door" for applications to access data, business logic, or functionality from back-end services, such as workloads running on Amazon EC2, code running on AWS Lambda, or any Web application. Amazon API Gateway handles all the tasks involved in accepting and processing up to hundreds of thousands of concurrent API calls, including traffic management, authorization and access control, monitoring, and API version management. Developers can now use custom authorizers on Amazon API Gateway to return additional fields in their authorization response. The custom authorizers can be used to authorize API requests to their backend using bearer token strategies such as OAuth. • https://aws.amazon.com/documentation/apigateway/
AWS Direct Connect	• AWS Direct Connect makes it easy to establish a dedicated network connection from a customer's premises to AWS. Using AWS Direct Connect, a customer can establish private connectivity between AWS and a data center, office, or colocation environment, which in many cases can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections. • http://aws.amazon.com/documentation/directconnect/
Developer Tools	
AWS CodeStar	• AWS CodeStar is a cloud-based development service that provides the tools that customers need to quickly develop, build, and deploy applications on AWS. With AWS CodeStar, customers can set up their entire continuous delivery toolchain in minutes, allowing them to start releasing code faster. AWS CodeStar makes it easy for a whole team to work together securely, with built-in role-based policies that allow customers to easily manage access and add owners, contributors, and viewers to projects. Each AWS CodeStar project comes with a unified project dashboard and integration with Atlassian JIRA software, a third-party issue tracking and project management tool. With the AWS CodeStar project dashboard, customers can easily track their entire software development process, from a backlog work item to production code deployment. • https://aws.amazon.com/documentation/codestar/
AWS CodeBuild	• AWS CodeBuild is a fully managed build service that compiles source code, runs tests, and produces software packages that are ready to deploy. With AWS CodeBuild, customers don't need to provision, manage, and scale their own build servers. AWS CodeBuild scales continuously and processes multiple builds concurrently, so builds are not left waiting in a queue. Customers can get started quickly by using prepackaged build environments or create custom build environments that use their own build tools. • https://aws.amazon.com/documentation/codebuild/

AWS Service (Hyperlink)	Description
AWS CodeDeploy	• AWS CodeDeploy is a service that automates code deployments to Amazon EC2 instances. AWS CodeDeploy makes it easier for customers to rapidly release new features, helps avoid downtime during deployment, and handles the complexity of updating applications. Customers can use AWS CodeDeploy to automate deployments, eliminating the need for error-prone manual operations, and the service scales with infrastructure so that customers can easily deploy to one Amazon EC2 instance or thousands. • http://aws.amazon.com/documentation/codedeploy/
AWS CodeCommit	• AWS CodeCommit is a secure, highly scalable, managed source control service that hosts private Git repositories. AWS CodeCommit eliminates the need for customers to operate their own source control system or worry about scaling its infrastructure. Customers can use AWS CodeCommit to store anything from code to binaries, and it supports the standard functionality of Git, allowing it to work seamlessly with existing Git-based tools. • http://aws.amazon.com/codecommit/
AWS CodePipeline	• AWS CodePipeline is a continuous delivery and release automation service that aids smooth deployments. Customers can design their development workflow for checking in code, building the code, deploying the application into staging, testing it, and releasing it to production. Customers can integrate third-party tools into any step of the release process, or they can use AWS CodePipeline as an end-to-end solution. • http://aws.amazon.com/codepipeline/
AWS X-Ray	• AWS X-Ray helps developers analyze and debug production, distributed applications, such as those built using a microservices architecture. With X-Ray, customers can understand how their application and its underlying services are performing to identify and troubleshoot the root cause of performance issues and errors. X-Ray provides an end-to-end view of requests as they travel through the application, and shows a map of the application's underlying components. Customers can use X-Ray to analyze both applications in development and in production, from simple three-tier applications to complex microservices applications consisting of thousands of services. • https://aws.amazon.com/documentation/xray/
Management	
Amazon CloudWatch	• Amazon CloudWatch is a service that enables customers to collect, view, and analyze metrics. Amazon CloudWatch lets customers programmatically retrieve monitoring data, view graphs, and set alarms to help troubleshoot, spot trends, and take automated action based on the state of a cloud environment. • http://aws.amazon.com/documentation/cloudwatch/
Amazon CloudWatch Events	• Monitor and automate action on Amazon EBS snapshots using Amazon CloudWatch Events. Amazon CloudWatch Events provide a stream of events describing changes to AWS resources. Amazon EBS CloudWatch Events fire

AWS Service (Hyperlink)	Description
	when a snapshot completes or when a snapshot has been shared with someone, which allows customers to automate and streamline their data backup workflows by eliminating the need to poll the snapshot API to track snapshot status. • https://aws.amazon.com/documentation/cloudwatch/
AWS CloudTrail	• With AWS CloudTrail, customers can get a history of AWS API calls for their account, including API calls made via the AWS Management Console, the AWS Software Development Kits (SDKs), the command line tools, and higher-level AWS Cloud services. Customers can also identify which users and accounts called AWS APIs for services that support AWS CloudTrail, the source IP address that the calls were made from, and when the calls occurred. Customers can integrate AWS CloudTrail into applications using the API, automate trail creation for their organization, check the status of their trails, and control how administrators turn AWS CloudTrail logging on and off. AWS CloudTrail supports Amazon S3 Data Events. Customers can record all API actions on Amazon S3 objects and receive detailed information. • http://aws.amazon.com/documentation/cloudtrail/
AWS Config	• AWS Config is a fully managed service that provides customers with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. With AWS Config customers can discover existing AWS resources, export a complete inventory of their AWS resources with all configuration details, and determine how a resource was configured at any point in time. Customers can use AWS Config to record configuration changes to software on their Amazon EC2 instances as well as Virtual Machines (VMs) or servers in their on-premises environment. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting. • http://aws.amazon.com/documentation/config/
AWS CloudFormation	• AWS CloudFormation gives developers and system administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion. Customers can use the sample templates for AWS CloudFormation or create their own templates to describe the AWS resources, and any associated dependencies or runtime parameters, required to run the application. • http://aws.amazon.com/documentation/cloudformation/
AWS OpsWorks	• AWS OpsWorks provides a simple and flexible way to create and manage stacks and applications. With AWS OpsWorks, customers can provision AWS resources, manage their configuration, deploy applications to those resources, and monitor their health. • http://aws.amazon.com/documentation/opsworks/
AWS Trusted Advisor	• AWS Trusted Advisor acts like a customized cloud expert, and it helps customers provision their resources by following best practices. AWS Trusted

AWS Service (Hyperlink)	Description
	Advisor inspects an AWS environment and finds opportunities to save money, improve system performance and reliability, or help close security gaps. • https://aws.amazon.com/premiumsupport/faqs/
AWS Systems Manager	• AWS Systems Manager allows customers to centralize operational data from multiple AWS services and automate tasks across AWS resources. Customers can create logical groups of resources such as applications, different layers of an application stack, or production versus development environments. With AWS Systems Manager, customers can select a resource group and view its recent API activity, resource configuration changes, related notifications, operational alerts, software inventory, and patch compliance status. AWS Systems Manager provides a central place to view and manage AWS resources, so customers can have complete visibility and control over their operations. • https://aws.amazon.com/documentation/systems-manager/
AWS Service Catalog	• AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows customers to centrally manage commonly deployed IT services, and helps them achieve consistent governance and meet compliance requirements, while enabling users to quickly deploy only the approved IT services they need. • https://aws.amazon.com/documentation/servicecatalog/
AWS Management Console	• The AWS Management Console provides customers with the ability to access and manage AWS Cloud services through a simple and intuitive web-based UI. Customers can also use the AWS Console mobile app to quickly view resources on the go. • http://docs.aws.amazon.com/awsconsolehelpdocs/latest/gsg/getting-started.html
AWS Command Line Tool	• The AWS Command Line Interface (CLI) is a unified tool to manage AWS Cloud services. With just one tool to download and configure, customers can control multiple AWS services from the command line and automate them through scripts. The AWS CLI introduces a new set of simple file commands for efficient file transfers to and from Amazon S3. • https://aws.amazon.com/documentation/cli/
AWS Personal Health Dashboard	• Customers can now receive notification and remediation guidance when AWS is experiencing events that may impact them. Available to all AWS customers, AWS Personal Health Dashboard provides a personalized view into the performance and availability of the AWS services a customer is using, as well as alerts that are automatically triggered by changes in the health of those services.
Media Services	

AWS Service (Hyperlink)	Description
Amazon Elastic Transcoder	• Amazon Elastic Transcoder lets customers convert media files that they have stored in Amazon S3 into media files in the formats required by consumer playback devices. For example, customers can convert large, high-quality digital media files into formats that users can play back on mobile devices, tablets, web browsers, and connected televisions. • http://aws.amazon.com/documentation/elastictranscoder/
Amazon Kinesis Video Streams	• Amazon Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), and other processing. Kinesis Video Streams automatically provisions and elastically scales all the infrastructure needed to ingest streaming video data from millions of devices. It also durably stores, encrypts, and indexes video data in streams, and allows customers to access their data through easy-to-use APIs. Kinesis Video Streams enables customers to quickly build computer vision and ML applications through integration with Amazon Rekognition Video and libraries for ML frameworks such as Apache MxNet, TensorFlow, and OpenCV. • https://aws.amazon.com/kinesis/video-streams/resources/
AWS Elemental MediaConvert	• AWS Elemental MediaConvert is a file-based video transcoding service with broadcast-grade features. It allows customers to easily create video-on-demand (VOD) content for broadcast and multiscreen delivery at scale. The service combines advanced video and audio capabilities with a simple web services interface and pay-as-you-go pricing. With AWS Elemental MediaConvert, customers can focus on delivering compelling media experiences without having to worry about the complexity of building and operating their own video processing infrastructure. • https://aws.amazon.com/mediaconvert/resources/
AWS Elemental MediaLive	• AWS Elemental MediaLive is a broadcast-grade live video processing service. It lets customers create high-quality video streams for delivery to broadcast televisions and internet-connected multiscreen devices, like connected TVs, tablets, smart phones, and set-top boxes. The service works by encoding live video streams in real-time, taking a larger-sized live video source and compressing it into smaller versions for distribution to viewers. With AWS Elemental MediaLive, customers can easily set up streams for both live events and 24x7 channels with advanced broadcasting features, high availability, and pay-as-you-go pricing. AWS Elemental MediaLive lets customers focus on creating compelling live video experiences for their viewers without the complexity of building and operating broadcast-grade video processing infrastructure. • https://aws.amazon.com/medialive/resources/
AWS Elemental MediaPackage	• AWS Elemental MediaPackage reliably prepares and protects video for delivery over the Internet. From a single video input, AWS Elemental MediaPackage creates video streams formatted to play on connected TVs, mobile phones, computers, tablets, and game consoles. It makes it easy to implement popular video features for viewers (start-over, pause, rewind, etc.),

AWS Service (Hyperlink)	Description
	like those commonly found on DVRs. AWS Elemental MediaPackage can also protect customer content using Digital Rights Management (DRM). AWS Elemental MediaPackage scales automatically in response to load, so viewers will always get a great experience without customers having to accurately predict in advance the capacity they'll need. • https://aws.amazon.com/mediapackage/resources/
AWS Elemental MediaStore	• AWS Elemental MediaStore is an AWS storage service optimized for media. It gives customers the performance, consistency, and low latency required to deliver live and on-demand video content. AWS Elemental MediaStore acts as the origin store in a video workflow. Its high-performance capabilities meet the needs of the most demanding media delivery workloads, combined with long-term, cost-effective storage. • https://aws.amazon.com/mediastore/resources/
AWS Elemental MediaTailor	• AWS Elemental MediaTailor lets video providers insert individually targeted advertising into their video streams without sacrificing broadcast-level quality-of-service. With AWS Elemental MediaTailor, viewers of live or on-demand video each receive a stream that combines content with ads personalized to them. But unlike other personalized ad solutions, with AWS Elemental MediaTailor entire stream—video and ads—are delivered with broadcast-grade video quality to improve the experience for viewers. • https://aws.amazon.com/mediatailor/resources/
Machine Learning	
Amazon SageMaker	• Amazon SageMaker is a fully-managed service that enables developers and data scientists to quickly and easily build, train, and deploy machine learning models at any scale. Amazon SageMaker removes the barriers that typically slow down developers who want to use machine learning. Amazon SageMaker includes modules that can be used together or independently to build, train, and deploy machine learning models. • https://aws.amazon.com/documentation/sagemaker/
Amazon Comprehend	• Amazon Comprehend is a natural language processing (NLP) service that uses machine learning to find insights and relationships in text. Amazon Comprehend identifies the language of the text; extracts key phrases, places, people, brands, or events; understands how positive or negative the text is; and automatically organizes a collection of text files by topic. The service constantly learns and improves from a variety of information sources, including Amazon.com product descriptions and consumer reviews—one of the largest natural language data sets in the world—to keep pace with the evolution of language. • https://aws.amazon.com/documentation/comprehend/
Amazon Lex	• Amazon Lex is a service for building conversational interfaces into any application using voice and text. Lex provides the advanced deep learning

AWS Service (Hyperlink)	Description
	functionalities of Automatic Speech Recognition (ASR) for converting speech to text, and Natural Language Understanding (NLU) to recognize the intent of the text, to enable customers to build applications with highly engaging user experiences and lifelike conversational interactions. With Amazon Lex, the same deep learning technologies that power Amazon Alexa are now available to any developer, enabling customers to quickly and easily build sophisticated, natural language, conversational bots ("chatbots"). • https://aws.amazon.com/lex/faqs/
Amazon Polly	• Amazon Polly is a service that turns text into lifelike speech. Polly lets customers create applications that talk, enabling customers to build entirely new categories of speech-enabled products. Amazon Polly is an Amazon AI service that uses advanced deep learning technologies to synthesize speech that sounds like a human voice. Amazon Polly includes 47 lifelike voices spread across 24 languages, so customers can select the ideal voice and build speech-enabled applications that work in many different countries. • https://aws.amazon.com/polly/developers/
Amazon Rekognition	• Amazon Rekognition is a service that makes it easy to add image analysis to applications. With Rekognition, customers can detect objects, scenes, and faces in images. Customers can also search and compare faces. Amazon Rekognition's API enables customers to quickly add sophisticated deep learning-based visual search and image classification to their applications. Amazon Rekognition uses deep neural network models to detect and label thousands of objects and scenes in images, and we are continually adding new labels and facial recognition features to the service. • https://aws.amazon.com/rekognition/developers/
Amazon Machine Learning	• Amazon Machine Learning makes it easy for developers to build smart applications, including applications for fraud detection, demand forecasting, targeted marketing, and click prediction. The powerful algorithms of Amazon Machine Learning create Machine Learning (ML) models by finding patterns in existing data. The service uses these models to process new data and generate predictions for an application. • https://aws.amazon.com/documentation/machine-learning/
Amazon Translate (in Preview)	• Amazon Translate is a neural machine translation service that delivers fast, high-quality, and affordable language translation. Neural machine translation is a form of language translation automation that uses machine learning and deep learning models to deliver more accurate and more natural sounding translation than traditional statistical and rule-based translation algorithms. Amazon Translate allows customers to easily translate large volumes of text efficiently, and to localize websites and applications for international users. • https://aws.amazon.com/translate/resources/
Amazon Transcribe	• Amazon Transcribe is an automatic speech recognition (ASR) service that makes it easy for developers to add speech to text capability to their

AWS Service (Hyperlink)	Description
	applications. Using the Amazon Transcribe API, customers can analyze audio files stored in Amazon S3 and have the service return a text file of the transcribed speech. Amazon Transcribe can be used for lots of common applications, including the transcription of customer service calls and generating subtitles on audio and video content. The service can transcribe audio files stored in common formats, like WAV and MP3, with time stamps for every word so customers can easily locate the audio in the original source by searching for the text. Amazon Transcribe is continually learning and improving to keep pace with the evolution of language. • https://aws.amazon.com/transcribe/resources/
AWS DeepLens	• AWS DeepLens is the world's first deep-learning enabled video camera for developers of all skill levels to grow their machine learning skills through hands-on computer vision tutorials, example code, and pre-built models. Customers can run the included sample projects as is, connect them with other AWS Cloud services, train a model in Amazon SageMaker and deploy it to AWS DeepLens, or extend the functionality by triggering a lambda function when an action takes place. Customers can even apply more advanced analytics on the cloud using Amazon Kinesis Video Streams and Amazon Rekognition video. AWS DeepLens provides the building blocks for machine learning needs. • https://aws.amazon.com/documentation/deeplens/
AWS Deep Learning AMIs	• The AWS Deep Learning AMIs provide machine learning practitioners and researchers with the infrastructure and tools to accelerate deep learning in the cloud, at any scale. Customers can quickly launch Amazon EC2 instances pre-installed with popular deep learning frameworks such as Apache MXNet and Gluon, TensorFlow, Microsoft Cognitive Toolkit, Caffe, Caffe2, Theano, Torch, Pytorch, and Keras to train sophisticated, custom AI models, experiment with new algorithms, or to learn new skills and techniques. • https://aws.amazon.com/documentation/dlami/
Apache MXNet on AWS	• Apache MXNet is a fast and scalable training and inference framework with an easy-to-use, concise API for machine learning. MXNet includes the Gluon interface that allows developers of all skill levels to get started with deep learning on the cloud, on edge devices, and on mobile apps. In just a few lines of Gluon code, customers can build linear regression, convolutional networks and recurrent LSTMs for object detection, speech recognition, recommendation, and personalization. • https://aws.amazon.com/documentation/mxnet/
TensorFlow on AWS	• TensorFlow™ enables developers to quickly and easily get started with deep learning in the cloud. The framework has broad support in the industry and has become a popular choice for deep learning research and application development, particularly in areas such as computer vision, natural language understanding and speech translation. Customers can get started using TensorFlow on AWS by launching the AWS Deep Learning AMI which

AWS Service (Hyperlink)	Description
	comes bundled with TensorFlow, as well as other popular deep learning frameworks such as Apache MXNet and Gluon, Caffe, Caffe2, Theano, Torch, Keras, and the Microsoft Cognitive Toolkit.
Analytics	
Amazon Athena	• Amazon Athena, a serverless query service that makes it easy to analyze data directly in Amazon S3 using standard SQL. With a few clicks in the AWS Management Console, customers can point Athena at their data stored in S3 and begin using standard SQL to run ad-hoc queries and get results in seconds. With Athena, there are no clusters to manage and tune, there is no infrastructure to setup, and customers pay only for the queries they run. Athena scales automatically, executing queries in parallel, so results are fast, even with large datasets and complex queries. • https://aws.amazon.com/athena/faqs/
Amazon EMR	• Amazon EMR is a web service that makes it easy to process large amounts of data efficiently. Amazon EMR uses Hadoop processing combined with several AWS products to perform such tasks as web indexing, data mining, log file analysis, machine learning, scientific simulation, and data warehousing. Customers configure policies to automatically add (scale out) and terminate (scale in) nodes in an Amazon EMR cluster programmatically. • http://aws.amazon.com/documentation/elasticmapreduce/
Amazon CloudSearch	• Amazon CloudSearch is a fully managed service in the cloud that makes it easy to set up, manage, and scale a search solution for a website. Amazon CloudSearch enables customers to search large collections of data such as web pages, document files, forum posts, or product information. With Amazon CloudSearch, customers can quickly add search capabilities to their websites without having to become a search expert or worry about hardware provisioning, setup, and maintenance. As the volume of data and traffic fluctuates, Amazon CloudSearch automatically scales to meet customers' needs. • http://aws.amazon.com/documentation/cloudsearch/
Amazon Elasticsearch Service	• Amazon Elasticsearch Service is a managed service that makes it easy to deploy, operate, and scale Elasticsearch in the AWS Cloud. Elasticsearch is a popular open-source search and analytics engine for use cases such as log analytics, real-time application monitoring, and click stream analytics. Customers can set up and configure their Amazon Elasticsearch cluster in minutes from the AWS Management Console. With Amazon Elasticsearch Service, customers get direct access to the Elasticsearch open-source API so that code and applications already being used with existing Elasticsearch environments will work seamlessly. • https://aws.amazon.com/documentation/elasticsearch-service/
Amazon Kinesis	• Amazon Kinesis makes it easy to collect, process, and analyze real-time, streaming data so that customers can get timely insights and react quickly to

AWS Service (Hyperlink)	Description
	new information. Amazon Kinesis offers key capabilities to cost-effectively process streaming data at any scale, along with the flexibility to choose the tools that best suit the requirements of the application. Amazon Kinesis enables customers to process and analyze data as it arrives and respond instantly instead of having to wait until all of the data is collected before the processing can begin. Amazon Kinesis offers four capabilities: • Kinesis Video Streams makes it easy to securely stream video from connected devices to AWS for analytics, machine learning (ML), and other processing. • Kinesis Data Streams enables customers to build custom, real-time applications that process data streams using popular stream processing frameworks. • Kinesis Data Firehose is the easiest way to capture, transform, and load data streams into AWS data stores for near real-time analytics with existing business intelligence tools. • Kinesis Data Analytics is the easiest way to process data streams in real time with SQL without having to learn new programming languages or processing frameworks. • http://aws.amazon.com/documentation/kinesis/
Amazon QuickSight	• Amazon QuickSight is a fast, cloud-powered business analytics service that makes it easy to build visualizations, perform ad-hoc analysis, and quickly get business insights from data. Using our cloud-based service customers can easily connect to data, perform advanced analysis, and create stunning visualizations and rich dashboards that can be accessed from any browser or mobile device. QuickSight enables organizations to scale their business analytics capabilities to hundreds of thousands of users, and delivers fast and responsive query performance by using a robust in-memory engine (SPICE). • https://aws.amazon.com/documentation/quicksight/
AWS Data Pipeline	• AWS Data Pipeline is a web service that helps customers reliably process and move data between different AWS compute and storage services, as well as on-premises data sources, at specified intervals. With AWS Data Pipeline, customers can regularly access their data where it's stored, transform and process it at scale, and efficiently transfer the results to AWS Cloud services such as Amazon S3, Amazon RDS, Amazon DynamoDB, and Amazon EMR. • http://aws.amazon.com/documentation/data-pipeline/
AWS Glue	• AWS Glue is a fully managed ETL service that makes it easy to move data stores. AWS Glue simplifies and automates the difficult and time-consuming data discovery, conversion, mapping, and job scheduling tasks. AWS Glue is integrated with Amazon S3, Amazon RDS, and Amazon Redshift and can connect to any JDBC-compliant data store. AWS Glue automatically crawls data sources, identifies data formats, and then suggests schemas and transformations, so customers don't have to spend time hand-coding data flows. AWS Glue is coming soon. • https://aws.amazon.com/documentation/glue/

AWS Service (Hyperlink)	Description
Security and Identify	
AWS IAM	• AWS Identity and Access Management (IAM) is a web service that enables AWS customers to manage users and user permissions. The service is targeted at organizations with multiple users or systems that use AWS products such as Amazon EC2, Amazon SimpleDB, and the AWS Management Console. With IAM, customers can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.AWS IAM roles and the AWS Security Token Service (STS) can be used to set up cross-account access between AWS accounts. When an IAM role in another AWS account is used to obtain cross-account access to services and resources in that account, AWS CloudTrail logs the cross-account activity. • http://aws.amazon.com/documentation/iam/
Amazon Cloud Directory	• Amazon Cloud Directory makes it easy to create highly flexible, scalable, and cost-effective directories. With Cloud Directory, customers can create directories for a variety of use cases, such as organizational charts, course catalogs, and device registries. While traditional directory solutions, such as Active Directory Lightweight Directory Services (AD LDS) and other LDAP-based directories, limit customers to a single hierarchy, Cloud Directory offers customers the flexibility to create directories with hierarchies that span multiple dimensions. Amazon Cloud Directory offers an extensible schema, designed to be shared across applications, and automatically scales to hundreds of millions of objects. • http://docs.aws.amazon.com/directoryservice/latest/APIReference/welcome.html
Amazon Cognito	• Amazon Cognito lets customers easily add user sign-up and sign-in to their mobile and web apps. With Amazon Cognito, customers also have the options to authenticate users through social identity providers such as Facebook, Twitter, or Amazon, with SAML identity solutions, or by using their own identity system. In addition, Amazon Cognito enables customers to save data locally on users' devices, allowing applications to work even when the devices are offline. Customers can then synchronize data across users' devices so that their app experience remains consistent regardless of the device they use. With Amazon Cognito, customers can focus on creating great app experiences instead of worrying about building, securing, and scaling a solution to handle user management, authentication, and sync across devices. • https://aws.amazon.com/documentation/cognito/
Amazon GuardDuty	• Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior to help customers protect their AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers. GuardDuty identifies suspected attackers through integrated threat intelligence feeds and uses machine learning to detect

AWS Service (Hyperlink)	Description
	anomalies in account and workload activity. When a potential threat is detected, the service delivers a detailed security alert to the GuardDuty console and AWS CloudWatch Events. This makes alerts actionable and easy to integrate into existing event management and workflow systems. • https://aws.amazon.com/guardduty/resources/
Amazon Inspector	• Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. • https://aws.amazon.com/documentation/inspector/
Amazon Macie	• Amazon Macie is an AI-powered security service that helps customers prevent data loss by automatically discovering, classifying, and protecting sensitive data stored in AWS. Amazon Macie uses ML to recognize sensitive data such as Personally Identifiable Information (PII) or intellectual property, assigns a business value, and provides visibility into where this data is stored and how it is being used in the organization. Amazon Macie continuously monitors data access activity for anomalies and delivers alerts when it detects risk of unauthorized access or inadvertent data leaks. • https://aws.amazon.com/documentation/macie/
AWS Certificate Manager	• AWS Certificate Manager is a service that lets customers easily provision, manage, and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS Cloud services. SSL/TLS certificates are used to secure network communications and establish the identity of websites over the Internet. • https://aws.amazon.com/documentation/acm/
AWS CloudHSM	• The AWS CloudHSM service helps customers meet corporate, contractual, and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) appliances within the AWS Cloud. With AWS CloudHSM, customers control the encryption keys and cryptographic operations performed by the HSM. • http://aws.amazon.com/documentation/cloudhsm/
AWS Directory Service	• AWS Directory Service is a managed service that allows customers to connect their AWS resources with an existing on-premises Microsoft Active Directory or to set up a new, standalone directory in the AWS Cloud. Connecting to an on-premises directory is easy, and when this connection is established, all users can access AWS resources and applications with their existing corporate credentials. • http://aws.amazon.com/documentation/directory-service/

AWS Service (Hyperlink)	Description
AWS KMS	• AWS Key Management Service (AWS KMS) is a managed service that makes it easy for customers to create and control the encryption keys used to encrypt their data. AWS KMS uses HSMs to protect the security of keys. AWS KMS is integrated with other AWS Cloud services, including Amazon EBS, Amazon S3, and Amazon Redshift. AWS KMS is also integrated with AWS CloudTrail to provide customers with logs of all key usage. • http://aws.amazon.com/documentation/kms/
AWS Organizations	• AWS Organizations offers policy-based management for multiple AWS accounts. With Organizations, customers can create groups of accounts and then apply policies to those groups. Organizations enables customers to centrally manage policies across multiple accounts, without requiring custom scripts and manual processes. Using AWS Organizations, customers can create Service Control Policies (SCPs) that centrally control AWS service use across multiple AWS accounts. Customers can also use Organizations to help automate the creation of new accounts through APIs. Organizations helps simplify the billing for multiple accounts by enabling customers to setup a single payment method for all the accounts in their organization through consolidated billing. • https://aws.amazon.com/documentation/organizations/
AWS Shield	• AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that protects web applications on AWS from DDoS attacks. AWS Shield Standard is available to all AWS customers at no additional cost, and protects applications from the most common, frequently occurring DDoS attacks. AWS Shield Advanced is available for a higher level of protection for applications on Elastic Load Balancing, Amazon CloudFront, and Amazon Route 53. With AWS Shield Advanced, customers also get access to AWS WAF at no additional cost. AWS Shield Advanced also provides 24x7 access to the DDoS Response Team (DRT) and DDoS Cost Protection, to protect their AWS bill against usage fee surges during mitigation of a DDoS attack. • https://aws.amazon.com/documentation/waf/
AWS WAF	• AWS WAF is a web application firewall that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. Also, AWS WAF includes a full-featured Application Programming Interface (API) that customers can use to automate the creation, deployment, and maintenance of web security rules. • https://aws.amazon.com/documentation/waf/
AWS Artifact	• AWS Artifact, available in the AWS Management Console, is a self-service audit artifact retrieval portal that provides our customers with on-demand access to AWS's compliance documentation. AWS Artifact provides on-demand access to AWS' security and compliance reports and select online agreements. Reports available in AWS Artifact include our SOC reports, PCI reports, and certifications from accreditation bodies across geographies and

AWS Service (Hyperlink)	Description
	compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Agreements available in AWS Artifact include the BAA and the NDA. • https://aws.amazon.com/documentation/artifact/
Mobile Services	
AWS Mobile Hub	• AWS Mobile Hub lets customers easily add and configure features for mobile apps, including user authentication, data storage, back-end logic, push notifications, content delivery, and analytics. AWS Mobile Hub gives customers easy access to testing on real devices, as well as analytics dashboards to track app usage, all from a single, integrated console. AWS Mobile Hub includes integration with Amazon Lex, so customers can build mobile apps that use speech and text to a mobile app. Amazon Lex lets customers use the technology that powers Amazon Alexa to create engaging speech- and text-based conversational bots in their own app. AWS Mobile Hub's SaaS Connectors make it easy to securely access data in third-party enterprise SaaS applications from a mobile apps. • https://aws.amazon.com/documentation/mobile-hub/
AWS Device Farm	• Improve the quality of iOS, Android, and web applications by testing against real phones and tablets in the AWS Cloud. AWS Device Farm is an app testing service that enables customers to test their iOS, Android, and Fire OS apps on real, physical phones and tablets that are hosted by AWS. The service allows customers to upload their own tests or use built-in, script-free compatibility tests. • https://aws.amazon.com/documentation/devicefarm/
Amazon Mobile Analytics	• With Amazon Mobile Analytics, customers can measure app usage and app revenue. By tracking key trends such as new vs. returning users, app revenue, user retention, and custom in-app behavior events, customers can make data-driven decisions to increase engagement and monetization for their app. Customers can view key charts in the Mobile Analytics console and automatically export app event data to Amazon S3 and Amazon Redshift to run custom analysis. • https://aws.amazon.com/documentation/mobileanalytics/
AWS Mobile SDK	• The AWS Mobile SDK helps customers build high quality mobile apps quickly and easily. It provides easy access to a range of AWS services, including Amazon Lambda, Amazon S3, Amazon DynamoDB, Amazon Mobile Analytics, Amazon Machine Learning, Elastic Load Balancing, Auto Scaling, and more. The AWS Mobile SDK includes libraries, code samples, and documentation for iOS, Android, Fire OS, and Unity so customers can build apps that deliver great experiences across devices and platforms. • https://aws.amazon.com/mobile/sdk/
Augmented Reality and Virtual Reality	

AWS Service (Hyperlink)	Description
Amazon Sumerian (in Preview)	• Amazon Sumerian lets customers create and run 3D, Augmented Reality (AR) and Virtual Reality (VR) applications. Customers can build immersive and interactive scenes that run on AR and VR, mobile devices, and web browser. Whether a customer is non-technical, a web or mobile developer, or has years of 3D development experience, getting started with Sumerian is easy. Customers can design scenes directly from their browser and, because Sumerian is a web-based application, customers can quickly add connections in their scenes to existing AWS Cloud services. • https://aws.amazon.com/documentation/sumerian/
Application Integration	
Amazon MQ	• Amazon MQ is a managed message broker service for Apache ActiveMQ that makes it easy to set up and operate message brokers in the cloud. Message brokers allow different software systems–often using different programming languages, and on different platforms–to communicate and exchange information. Amazon MQ manages the administration and maintenance of ActiveMQ, a popular open-source message broker. The underlying infrastructure is automatically provisioned for high availability and message durability to support customers' reliability of applications. With Amazon MQ, customers get direct access to the ActiveMQ console and industry standard APIs and protocols for messaging, including JMS, NMS, AMQP, STOMP, MQTT, and WebSockets. • https://aws.amazon.com/amazon-mq/resources/
Amazon SQS	• Amazon Simple Queue Service (Amazon SQS) is a messaging queue service that handles messages or workflows between other components in a system. • http://aws.amazon.com/documentation/sqs/
Amazon SNS	• Amazon Simple Notification Service (Amazon SNS) is a fast, flexible, fully managed push notification service that lets customers send individual messages or to fan-out messages to large numbers of recipients. Amazon SNS makes it simple and cost effective to send push notifications to mobile device users and email recipients or even send messages to other distributed services. With Amazon SNS, customers can send notifications to Apple, Google, Fire OS, and Windows devices, as well as to Android devices in China with Baidu Cloud Push. Customers can use SNS to send SMS messages to mobile device users worldwide. • https://aws.amazon.com/documentation/sns/
AWS AppSync (in Preview)	• AWS AppSync automatically updates the data in web and mobile applications in real time, and updates data for offline users as soon as they reconnect. AppSync makes it easy to build collaborative mobile and web applications that deliver responsive, collaborative user experiences. • Customers can use AWS AppSync to build native mobile and web apps with iOS, Android, JavaScript and React Native. Get started by going to the AWS AppSync console, specify the data for an app with simple code statements, and

AWS Service (Hyperlink)	Description
	AppSync will manage everything needed to store, process, and retrieve the data for the application. • https://aws.amazon.com/documentation/appsync/
AWS Step Functions	• AWS Step Functions makes it easy to coordinate the components of distributed applications and microservices using visual workflows. Building applications from individual components lets customers scale and change applications quickly. AWS Step Functions is a reliable way to coordinate components and step through the functions of application. AWS Step Functions provides a graphical console to arrange and visualize the components, which makes it simple to build and run multi-step applications. AWS Step Functions automatically triggers and tracks each step, and retries when there are errors, so the application executes in order and as expected. The state of each step is logged, so when things do go wrong, customers can diagnose and debug problems quickly. Customers can change and add steps without even writing code, so they can easily evolve their application and innovate faster. • https://aws.amazon.com/documentation/step-functions/
Amazon SWF	• Amazon Simple Workflow Service (Amazon SWF) makes it easy to build applications that coordinate work across distributed components. In Amazon SWF, a task represents a logical unit of work that is performed by a component of an application. Coordinating tasks across the application involves managing inter-task dependencies, scheduling, and concurrency in accordance with the logical flow of the application. Amazon SWF gives customers full control over implementing tasks and coordinating them without having to manage underlying complexities such as tracking their progress and maintaining their state. • http://aws.amazon.com/documentation/swf/
Amazon FPS	• Amazon Flexible Payments Service (Amazon FPS) facilitates the digital transfer of money between any two entities (humans or computers). • https://payments.amazon.com/developer
Customer Engagement	
Amazon Connect	• Amazon Connect is a self-service, cloud-based contact center service that makes it easy for any business to deliver better customer service at lower cost. Amazon Connect is based on the same contact center technology used by Amazon customer service associates around the world to power millions of customer conversations. The self-service graphical interface in Amazon Connect makes it easy for non-technical users to design contact flows, manage agents, and track performance metrics—no specialized skills required. Customers pay by the minute for Amazon Connect usage plus any associated telephony services. • https://aws.amazon.com/documentation/connect/

AWS Service (Hyperlink)	Description
Amazon Pinpoint	• Amazon Pinpoint makes it easy to run targeted campaigns to drive user engagement in mobile apps. Amazon Pinpoint helps customers understand user behavior, define which users to target, determine which messages to send, schedule the best time to deliver the messages, and then track the results of a campaign. Amazon Pinpoint is built to scale with an app, enabling customers to collect and process billions of events per day, and send millions of targeted push notifications to users. • https://aws.amazon.com/pinpoint/faqs/
Amazon SES	• Amazon Simple Email Service (Amazon SES) is a cost-effective email service built on the reliable and scalable infrastructure that Amazon.com developed to serve its own customer base. With Amazon SES, customers can send and receive email with no required minimum commitments. Amazon SES offers dedicated IP addresses, which enable customers to manage the reputation of the IP addresses that Amazon SES uses to send their email. Dedicated IP addresses are Amazon SES IP addresses that are reserved exclusively for email sending. • http://aws.amazon.com/documentation/ses/
Business Productivity	
Alexa for Business	• Alexa for Business allows organizations of all sizes to introduce Alexa to their workplace. With Alexa for Business, customers can use the Alexa they know as an intelligent assistant to stay organized and focus on the work that matters. Alexa helps workers be more productive as they move throughout their day, at home and at their desks as enrolled users with personal devices, and in conference rooms, copy rooms or other shared spaces with shared devices. Alexa for Business includes the tools and controls that administrators need to deploy and manage shared Alexa devices, skills, and users at scale. • https://aws.amazon.com/documentation/a4b/
Amazon Chime	• Amazon Chime is a high-quality communications service that transforms online meetings with an easy-to-use app which works seamlessly across all devices. With Amazon Chime, customers can schedule and attend online meetings and video conferences, and chat, call, and collaborate, inside and outside of their organization, all with a single app. Now customers can work productively from wherever they are. • https://aws.amazon.com/documentation/chime/
Amazon WorkDocs	• Amazon WorkDocs is a fully managed, secure enterprise storage and sharing service with strong administrative controls and feedback capabilities to help improve user productivity. Users can comment on files, send them to others for feedback, and upload new versions without having to resort to emailing multiple versions of their files as attachments. Amazon WorkDocs default storage quota is 1TB. • http://aws.amazon.com/documentation/workdocs/

AWS Service (Hyperlink)	Description
Amazon WorkMail	• Amazon WorkMail is a secure, managed business email and calendar service with support for existing desktop and mobile email clients. Amazon WorkMail gives users the ability to seamlessly access their email, contacts, and calendars using Microsoft Outlook, their web browser, or their native iOS and Android email applications. Amazon WorkMail offers SMTP journaling, which allows customers to record all email communication sent or received by their Amazon WorkMail organization. Journaling allows customers to integrate with third-party compliance solutions for email archiving and e-discovery, allowing them to meet data security and information protection policies. • https://aws.amazon.com/documentation/workmail/
Desktop and Application Streaming	
Amazon WorkSpaces	• Amazon WorkSpaces allows customers to easily provision cloud-based desktops that allow users to access the documents, applications, and resources they need with the device of their choice, including laptops, iPad, Kindle Fire, or Android tablets. With a few clicks in the AWS Management Console, customers can provision a high-quality cloud desktop experience for any number of users at a highly competitive cost that is half the cost of most Virtual Desktop Infrastructure (VDI) solutions. Amazon WorkSpaces offers bundles that come with a Windows 10 desktop experience, powered by Windows Server 2016. Amazon WorkSpaces also provides Graphics bundles that offer a virtual cloud desktop with a high-end GPU that supports engineering, design, and architectural applications. • http://aws.amazon.com/documentation/workspaces/
Amazon AppStream	• The Amazon AppStream web service deploys application on AWS infrastructure and streams input and output between the application and devices such as personal computers, tablets, and mobile phones. The application's processing occurs in the cloud, so it can scale to handle vast computational loads. Devices need only display output and return user input, so the client application on the device can be lightweight in terms of file size and processing requirements. • http://aws.amazon.com/documentation/appstream/
Amazon App Stream 2.0	• Amazon AppStream 2.0 is a fully managed, secure application streaming service that allows customers to stream desktop applications from AWS to any device, without rewriting them. AppStream 2.0 provides users with instant-on access to the applications they need, and a responsive, fluid user experience running in an HTML5 web browser. • https://aws.amazon.com/appstream2/resources/
Internet of Things	
AWS IoT Core	• AWS IoT Core is a managed cloud platform that lets connected devices easily and securely interact with cloud applications and other devices. AWS IoT Core can support billions of devices and trillions of messages, and can process and

AWS Service (Hyperlink)	Description
	route those messages to AWS endpoints and to other devices reliably and securely. With AWS IoT Core, applications can keep track of and communicate with all devices, all the time, even when they aren't connected. AWS IoT Core makes it easy to use AWS Cloud services to build IoT applications that gather, process, analyze, and act on data generated by connected devices, without having to manage any infrastructure. • https://aws.amazon.com/iot-core/resources/
Amazon FreeRTOS	• Amazon FreeRTOS (FreeRTOS) is an operating system that makes microcontroller-based edge devices easy to program, deploy, secure, and maintain. Amazon FreeRTOS is based on the FreeRTOS kernel, the popular open source operating system for microcontrollers, and includes software libraries that make it easy to securely connect devices locally, to the cloud, and update them remotely. The Amazon FreeRTOS console enables customers to easily select and download the software components relevant to their use case. • https://aws.amazon.com/documentation/freertos/
AWS Greengrass	• AWS Greengrass is software that lets customers run local compute, messaging, and data caching for connected devices in a secure way. With AWS Greengrass, connected devices can run AWS Lambda functions, keep device data in sync, and communicate with other devices securely, even when not connected to the Internet. Using AWS Lambda, AWS Greengrass ensures that IoT devices can respond quickly to local events, operate with intermittent connections, and minimize the cost of transmitting IoT data to the cloud. • https://aws.amazon.com/greengrass/faqs/
AWS IoT 1-Click	• AWS IoT 1-Click is a new service that makes it easy for simple devices to trigger actions like Lambda functions. With AWS IoT 1-Click, simple devices are ready to securely connect to AWS IoT Core right out of the box. This makes it easy for developers to deploy these devices into their IoT applications and for device manufacturers to register their simple devices with AWS IoT Core at the factory. • Not available at this time
AWS IoT Analytics	• AWS IoT Analytics is a fully-managed IoT analytics service that collects, pre-processes, enriches, stores, and analyzes IoT device data at scale. IoT Analytics can perform simple ad hoc queries as well as complex analysis, and is a simpler way to run IoT analytics for use cases such as understanding the performance of devices, predicting device failures, and machine learning. It is designed specifically for IoT and automatically captures and stores the message timestamp so it is easy to perform time-series analysis. IoT Analytics can also enrich the data with device-specific metadata such as device type and location using the AWS IoT registry. IoT Analytics stores data in an IoT-optimized data store so customers can run queries on large datasets. • Not available at this time

AWS Service (Hyperlink)	Description
AWS IoT Button	• The AWS IoT Button is a programmable button based on the Amazon Dash Button hardware. This simple Wi-Fi device is easy to configure and designed for developers to get started with AWS IoT Core, AWS Lambda, Amazon DynamoDB, Amazon SNS, and many other AWS without writing device-specific code. • Not available at this time
AWS IoT Device Defender	• AWS IoT Device Defender is a fully managed service that helps customers secure their fleet of IoT devices. AWS IoT Device Defender continuously audits the security policies associated with devices to make sure that they aren't deviating from security best practices. AWS IoT Device Defender makes it easy to maintain and enforce security policies, such as ensuring device identity, authenticating and authorizing devices, and encrypting device data. • Not available at this time
AWS IoT Device Management	• AWS IoT Device Management is a service that makes it easy to securely onboard, organize, monitor, and remotely manage IoT devices at scale throughout their lifecycle. Customers can use IoT Device Management to upload and view device information and configuration, organize their device inventory, monitor their fleet of devices, and remotely manage devices deployed across many locations including updating device software Over-The-Air (OTA). With IoT Device Management, customers can scale their device fleets and reduce the cost and effort of managing large IoT device deployments. • https://aws.amazon.com/documentation/iot-device-management/
Game Development	
Amazon Lumberyard (Beta)	• Amazon Lumberyard is a free, cross-platform, 3D game engine for customers to create the highest-quality games, connect their games to the vast compute and storage of the AWS Cloud, and engage fans on Twitch. By starting game projects with Lumberyard, customers can spend more of their time creating great gameplay and building communities of fans and less time on the undifferentiated heavy lifting of building a game engine and managing server infrastructure. • https://aws.amazon.com/documentation/lumberyard/
Amazon GameLift	• Amazon GameLift, a managed service for deploying, operating, and scaling session-based multiplayer games, reduces the time required to build a multiplayer backend from thousands of hours to just minutes. Available for developers using Amazon Lumberyard, Amazon GameLift is built on AWS's highly available cloud infrastructure and allows customers to quickly scale high-performance game servers up and down to meet player demand—without any additional engineering effort or upfront costs. • https://aws.amazon.com/documentation/gamelift/

AWS Service (Hyperlink)	Description
Software	
AWS Marketplace	• AWS Marketplace is an online store that helps customers find, buy, and immediately start using the software and services they need to build products and run their businesses. • https://aws.amazon.com/marketplace/help/
AWS Support	
AWS Support	• AWS Support is a one-on-one, fast-response support channel that is staffed 24x7x365 with experienced technical support engineers to help customers of all sizes and technical abilities successfully use the products and features provided by AWS. • https://aws.amazon.com/documentation/aws-support/

30. APPENDIX: SERVICENOW SUBSCRIPTION GUIDE-SLA (AS OF 6-29-2018)

servicenow

SUBSCRIPTION SERVICE AGREEMENT

SUBSCRIPTION SERVICE AGREEMENT

This Subscription Service Agreement (including the Subscription Service Guide, attached hereto) ("**Agreement**") is made between the ServiceNow entity ("**ServiceNow**") and the customer entity ("**Customer**") on the ordering document and becomes effective on the last signature date of the ordering document issued by ServiceNow ("**Effective Date**").

The Agreement is deemed to include the General Terms and Conditions below, the Subscription Service Guide attached as Exhibit A.1 (which includes Exhibit A.2 - Customer Support Policy, Exhibit A.3 - Upgrades and Updates, Exhibit A.4 - Data Processing Addendum, and Exhibit A.5 - Data Security Guide), and any other terms expressly referenced herein or in other incorporated documents, all of which are expressly deemed incorporated in the Agreement by this reference. The Subscription Service Guide is posted on https://www.servicenow.com/schedules.html and incorporated herein by reference.

Pursuant to a separate transaction between Customer and ServiceNow's authorized reseller ("**Reseller**"), Customer has purchased from Reseller certain services to be delivered by ServiceNow. This Agreement specifies the terms and conditions under which those services will be provided, apart from price, payment and other terms specified in the separate agreement between Customer and Reseller.

GENERAL TERMS AND CONDITIONS

1. DEFINITIONS

1.1 "**Affiliates**" means any person or entity directly or indirectly Controlling, Controlled by, or under common Control with a party, where "**Control**" means the legal power to direct or cause the direction of the general management of the company, partnership, or other legal entity.

1.2 "**Ancillary Software**" means software licensed by ServiceNow to Customer that is deployed on machines operated by or for Customer to facilitate operation of the Subscription Service or interoperation of the Subscription Service with other software, hardware, or services. Ancillary Software may include code that is licensed under third-party license agreements, including open source made available or provided with the Ancillary Software.

1.3 "**Claim**" means any third-party suit, claim, action, or demand.

1.4 "**Confidential Information**" means: **(a)** ServiceNow Core Technology (which is Confidential Information of ServiceNow); **(b)** Customer Data and Customer Technology (which is Confidential Information of Customer); **(c)** any information of a party that is disclosed in writing or orally and is designated as *Confidential* or *Proprietary* at time of disclosure (and, for oral disclosures, summarized in writing within 30 days of initial disclosure and delivered in written summary form to the receiving party), or that, due to the nature of the information or circumstances of disclosure, receiving party would understand it to be disclosing party's confidential information; and **(d)** the specific terms of this Agreement, any Use Authorization, any SOW, and any amendment or attachment to any of these, between the parties (which will be deemed Confidential Information of both parties). Confidential Information excludes any information that: **(i)** is or becomes generally known to the public through no fault or breach of this Agreement by receiving party; **(ii)** was already rightfully in receiving party's possession, without restriction on use or disclosure, when receiving party received it under this Agreement; **(iii)** is independently developed by receiving party without use of disclosing party's Confidential Information; or **(iv)** was or is rightfully obtained by receiving party, without restriction on use or disclosure, from a third party not under a duty of confidentiality to disclosing party.

1.5 "**Customer Data**" means electronic data uploaded by or for Customer or Customer's agents, employees, or contractors, and processed in the Subscription Service, excluding ServiceNow Core Technology.

1.6 "**Customer Technology**" means software, methodologies, templates, business processes, documentation, or other material originally authored, invented, or otherwise created by Customer (or on Customer's behalf, other than by ServiceNow or at ServiceNow's direction) for use with the Subscription Service, excluding ServiceNow Core Technology.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

1.7 "**Deliverable**" means anything that is created by or on behalf of ServiceNow for Customer in the performance of Professional Services.

1.8 "**Documentation**" means the then-current ServiceNow product documentation relating to the operation and use of the Subscription Service or Ancillary Software published by ServiceNow at https://docs.servicenow.com or its successor website. Documentation includes technical program or interface documentation, user manuals, operating instructions, and release notes.

1.9 "**Intellectual Property Rights**" means all intellectual property or other proprietary rights worldwide, including patents, copyrights, trademarks, moral rights, trade secrets, and any other intellectual or industrial property, including registrations, applications, renewals, and extensions of such rights.

1.10 "**Law**" means any applicable law, rule, statute, decree, decision, order, regulation, judgment, code, and requirement of any government authority (federal, state, local, or international) having jurisdiction.

1.11 "**Newly Created IP**" means Intellectual Property Rights in the inventions or works of authorship that are made by ServiceNow specifically for Customer in the course of performing Professional Services for Customer that are expressly identified as "Newly Created IP" in an SOW, excluding ServiceNow Core Technology.

1.12 "**Product Overview**" means ServiceNow's published description of its products and their functionalities, solely to the extent attached to or expressly referenced in a Use Authorization.

1.13 "**Professional Services**" means any consulting, development, or educational services provided by or on behalf of ServiceNow pursuant to an agreed SOW or Service Description.

1.14 "**Service Description**" means the written description for a packaged Professional Service, attached to or referenced in a Use Authorization.

1.15 "**ServiceNow Core Technology**" means: **(a)** the Subscription Service, Ancillary Software, Documentation, and technology and methodologies (including products, software tools, hardware designs, algorithms, templates, software (in source and object forms), architecture, class libraries, objects, and documentation) created by or for, or licensed to, ServiceNow; and **(b)** updates, upgrades, improvements, configurations, extensions, and derivative works of the foregoing and related technical or end user documentation or manuals.

1.16 "**ServiceNow Products**" means, collectively, the Subscription Service, Ancillary Software, Documentation, and Deliverables.

1.17 "**SOW**" means a statement of work that describes scoped Professional Services.

1.18 "**Subscription Service**" means the ServiceNow software-as-a-service offering ordered by Customer under a Use Authorization.

1.19 "**Subscription Term**" means the period of authorized access to and use of the Subscription Service, as set forth in a Use Authorization.

1.20 "**Use Authorization**" means a written document provided to Customer specifying the services that Customer has purchased, along with the term and scope of the authorized use thereof.

2. ACCESS AND USE RIGHTS; RESTRICTIONS; PROVISION OF PROFESSIONAL SERVICES

2.1 ACCESS AND USE RIGHTS. For each Subscription Term, ServiceNow grants the access and use rights set forth in this Section 2 for the ServiceNow Core Technology described in that Use Authorization.

2.1.1. SUBSCRIPTION SERVICE. Subject to the terms of this Agreement, ServiceNow authorizes Customer to access and use the Subscription Service during the Subscription Term stated in the applicable Use Authorization, solely for its internal business purposes in accordance with the Documentation. Customer will not otherwise access or use the Subscription Service in a manner that exceeds Customer's authorized access and use rights as set forth in this Agreement and the applicable Use Authorization.

2.1.2. ANCILLARY SOFTWARE. ServiceNow grants Customer a limited, personal, worldwide, non-sublicensable, non-transferable (except as set forth in Section 12.1 (Assignment)), non-exclusive, royalty-free license during the Subscription Term to install and execute Ancillary Software on machines operated by or for Customer, solely to facilitate Customer's authorized access to and use of the Subscription Service.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

2.2 RESTRICTIONS. With respect to the ServiceNow Core Technology, Customer will not (and will not permit others to): **(a)** use it in excess of contractual usage limits (including as set forth in a Use Authorization), or in a manner that circumvents usage limits or technological access control measures; **(b)** license, sub-license, sell, re-sell, rent, lease, transfer, distribute, time share, or otherwise make any of it available for access by third-parties, except as may otherwise be expressly stated in a Use Authorization; **(c)** access it for the purpose of developing or operating products or services for third-parties in competition with the ServiceNow Core Technology; **(d)** disassemble, reverse engineer, or decompile it; **(e)** copy, create derivative works based on, or otherwise modify it, except as may be otherwise expressly stated in this Agreement; **(f)** remove or modify a copyright or other proprietary rights notice in it; **(g)** use it to reproduce, distribute, display, transmit, or use material protected by copyright or other Intellectual Property Right (including the rights of publicity) without first obtaining permission of the owner; **(h)** use it to create, use, send, store, or run viruses or other harmful computer code, files, scripts, agents, or other programs, or otherwise engage in a malicious act or disrupt its security, integrity, or operation; or **(i)** access or disable any ServiceNow or third-party data, software, or network (other than Customer's instance of the Subscription Service under this Agreement). Before Customer engages in any of the foregoing acts that it believes it may be entitled to, it will provide ServiceNow with 30-days' prior notice to legalnotices@servicenow.com, and reasonably requested information to allow ServiceNow to assess Customer's claim. ServiceNow may, in its discretion, provide alternatives that reduce adverse impacts on ServiceNow's Intellectual Property Rights or other rights.

2.3 PROVISION OF PROFESSIONAL SERVICES. Customer and ServiceNow may enter into one or more SOWs or Use Authorizations subject to this Agreement, and which may incorporate one or more Service Descriptions for the provision of Professional Services. ServiceNow will perform the Professional Services, subject to the fulfillment of any responsibilities and payments due from Customer, as stated in the SOW or the Use Authorization.

3. ORDERING

3.1 RESELLER ORDERS. Customer shall order and purchase the Subscription Service and Professional Services directly from Reseller pursuant to a separate agreement specifying price, payment and other commercial terms. ServiceNow is not a party to such separate agreement but will provide the purchased services pursuant to this Agreement. For each order, Reseller or ServiceNow will provide Customer with a Use Authorization for Customer to sign and return to ServiceNow. ServiceNow will have no obligation to provide services unless and until it has received a Use Authorization signed by Customer. Reseller is not authorized to make any changes to this Agreement (including any Use Authorizations issued hereunder) or bind ServiceNow to any additional or different terms or conditions. Additional orders for ServiceNow products or services may be placed either through Reseller or ServiceNow, provided that if Customer places an order directly through ServiceNow, Customer shall sign an addendum to this Agreement setting forth pricing, payment and other commercial terms between Customer and ServiceNow.

3.2 USE VERIFICATION. ServiceNow or Reseller may remotely review Customer's use of the Subscription Service, and on ServiceNow or Reseller's written request, Customer will provide reasonable assistance to verify Customer's compliance with the Agreement, and access to and use of the Subscription Service. If ServiceNow or Reseller determines that Customer has exceeded its permitted access and use rights to the Subscription Service, ServiceNow will notify Customer and within 30 days thereafter Customer shall either: **(a)** disable any unpermitted use, or **(b)** purchase additional subscriptions commensurate with Customer's actual use.

4. INTELLECTUAL PROPERTY

4.1 SERVICENOW OWNERSHIP. As between the parties, ServiceNow and its licensors exclusively own all right, title, and interest in and to all Intellectual Property Rights in the ServiceNow Core Technology, notwithstanding anything in this Agreement purportedly to the contrary. Except for the access and use rights, and licenses expressly granted in Section 2 (Access and Use Rights; Restrictions; Provision of Professional Services) of this Agreement, ServiceNow, on behalf of itself and its licensors, reserves all rights in the ServiceNow Core Technology and does not grant Customer any rights (express, implied, by estoppel, through exhaustion, or otherwise). Any ServiceNow Core Technology delivered to Customer or to which Customer is given access shall not be deemed to have been sold, even if, for convenience, ServiceNow makes reference to words such as "sale" or "purchase" in the applicable Use Authorization or other documents.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

4.2 CUSTOMER OWNERSHIP. As between the parties, Customer and its licensors will retain all right, title, and interest in and to all Intellectual Property Rights in Customer Data and Customer Technology. Customer hereby grants to ServiceNow a royalty-free, fully-paid, non-exclusive, non-transferrable (except as set forth in Section 12.1 (Assignment)), worldwide, right to use Customer Data and Customer Technology solely to provide and support the ServiceNow Products.

4.3 FEEDBACK. ServiceNow encourages Customer to provide suggestions, proposals, ideas, recommendations, or other feedback regarding improvements to the ServiceNow Products (collectively, "**Feedback**"). If Customer provides such Feedback, Customer grants to ServiceNow a royalty-free, fully paid, sub-licensable, transferable (notwithstanding Section 12.1 (Assignment)), non-exclusive, irrevocable, perpetual, worldwide right and license to use, license, and commercialize Feedback (including by incorporation of such Feedback into ServiceNow Core Technology) without restriction.

4.4 PROFESSIONAL SERVICES. Subject to this Section 4.4, ServiceNow assigns (and in the future is deemed to have assigned) to Customer any Newly Created IP upon payment in full by Customer for the Professional Service under which the Newly Created IP was created. If any ServiceNow Core Technology is incorporated into a Deliverable, ServiceNow grants to Customer a non-exclusive, royalty-free, non-transferable (except as set forth in Section 12.1 (Assignment)), non-sublicensable worldwide license to use the ServiceNow Core Technology incorporated into the Deliverable in connection with the Subscription Service as contemplated under this Agreement during the applicable Subscription Term. Nothing in this Agreement shall be deemed to restrict or limit ServiceNow's right to perform similar Professional Services for any other party or to assign any employees or subcontractors to perform similar Professional Services for any other party or to use any information incidentally retained in the unaided memories of its employees providing Professional Services.

5. WARRANTIES; DISCLAIMER OF WARRANTIES

5.1 LIMITED SUBSCRIPTION SERVICE WARRANTY. ServiceNow warrants that, during the Subscription Term, Customer's production instance of the Subscription Service will materially conform to the Product Overview. To submit a warranty claim under this Section 5.1, Customer will submit a support request to resolve the non-conformity as provided in the Subscription Service Guide. If the non-conformity persists without relief more than 30 days after notice of a warranty claim provided to ServiceNow under this Section 5.1, then Customer may terminate the affected Subscription Service, and submit to Reseller a claim for refund to Customer for any prepaid subscription fees covering that part of the applicable Subscription Term for the affected Subscription Service remaining after the effective date of termination. Notwithstanding the foregoing, this warranty will not apply to any non-conformity due to a modification of or defect in the Subscription Service that is made or caused by any person other than ServiceNow or a person acting at ServiceNow's direction. **This Section 5.1 sets forth Customer's exclusive rights and remedies (and ServiceNow's sole liability) in connection with this warranty.**

5.2 LIMITED PROFESSIONAL SERVICES WARRANTY. ServiceNow warrants that the Professional Services will be performed in a competent and workmanlike manner, in accordance with accepted industry standards and practices and all material requirements set forth in the SOW or Service Description. Customer will notify ServiceNow of any breach within 30 days after performance of the non-conforming Professional Services. On receipt of such notice, ServiceNow, at its option, will either use commercially reasonable efforts to re-perform the Professional Services in conformance with these warranty requirements or will terminate the affected Professional Services, whereupon Customer may submit to Reseller a claim for a refund of any any amounts paid for the nonconforming Professional Services. **This Section 5.2 sets forth Customer's exclusive rights and remedies (and ServiceNow's sole liability) in connection with this warranty.**

5.3 DISCLAIMER OF WARRANTIES. **Except for the warranties expressly stated in this Section 5, to the maximum extent allowed by Law, ServiceNow disclaims all warranties of any kind (express, implied, statutory, or otherwise, oral or written, including warranties of merchantability, accuracy, title, non-infringement, or fitness for a particular purpose, and any warranties arising from usage of trade, course of dealing, or course of performance). Without limiting the foregoing, ServiceNow specifically does not warrant that the ServiceNow Products will meet the requirements of Customer or others or will be accurate or operate without interruption or error. Customer acknowledges that in entering this Agreement, it has not relied on any promise, warranty, or representation not expressly set forth in this Agreement.**

servicenow

SUBSCRIPTION SERVICE AGREEMENT

6. CONFIDENTIAL INFORMATION

6.1 CONFIDENTIALITY OBLIGATIONS. The recipient of Confidential Information will: **(a)** at all times protect it from unauthorized disclosure with the same degree of care that it uses to protect its own confidential information, and in no event use less than reasonable care; and **(b)** not use it except to the extent necessary to exercise rights or fulfill obligations under this Agreement. Each party will limit the disclosure of the other party's Confidential Information to those of its employees and contractors and the employees and contractors of its Affiliates with a need to access such Confidential Information for a party's exercise of its rights and obligations under this Agreement, and then only to employees and contractors subject to binding disclosure and use restrictions at least as protective as those in this Agreement. Each party's obligations under this Section 6 will remain in effect during, and for three years after termination of, this Agreement. Receiving party will, at disclosing party's request, return all originals, copies, reproductions, and summaries of Confidential Information and other tangible materials and devices provided to receiving party as Confidential Information, or at disclosing party's option, certified destruction of the same. Provisions for return of Customer Data are set forth in Section 11.2 (Return of Customer Data).

6.2 THIRD PARTY REQUESTS. This Agreement will not be construed to prevent receiving party from disclosing the disclosing party's Confidential Information to a court, or governmental body pursuant to a valid court order, Law, subpoena, or regulation, provided that the receiving party: **(a)** gives prompt notice (or the maximum notice permitted under Law) before making the disclosure, unless prohibited by Law; **(b)** provides reasonable assistance to disclosing party in any lawful efforts by disclosing party to resist or limit the disclosure of such Confidential Information; and **(c)** discloses only that portion of disclosing party's Confidential Information that is legally required to be disclosed. In addition, receiving party will cooperate and assist disclosing party, at disclosing party's cost, in relation to any such request and any response to any such communication.

7. INDEMNIFICATION

7.1 BY SERVICENOW.

7.1.1. SERVICENOW OBLIGATION. Subject to the limitations in this Section 7, ServiceNow will: **(a)** defend Customer, and its and their officers, directors, and employees against any Claim: **(i)** to the extent alleging that any ServiceNow Core Technology accessed or used in accordance with this Agreement infringes any third-party patent, copyright, or trademark, or misappropriates any third-party trade secret; or **(ii)** to the extent alleging that ServiceNow's personnel when onsite at Customer's premises caused death, bodily harm, or damage to tangible personal property due to their negligence or willful misconduct; and **(b)** pay any settlement amount or any court-ordered award of damages, under the forgoing subsections (a)(i) and (ii) to the extent arising from such Claim.

7.1.2. MITIGATION. To the extent any Claim alleges any part of the ServiceNow Core Technology infringes any third-party patent, copyright, or trademark, or misappropriates any third-party trade secret, ServiceNow may: **(a)** contest the Claim; **(b)** obtain permission from the claimant for Customer's continued use of its instance of the Subscription Service or any applicable ServiceNow Core Technology; **(c)** avoid such Claim by replacing or modifying Customer's access to and use of its instance of the Subscription Service or any applicable ServiceNow Core Technology as long as ServiceNow provides a substantially similar Subscription Service; or, if ServiceNow determines the foregoing (a), (b), and (c) are not commercially practicable, then **(d)** terminate Customer's access to and use of the affected Subscription Service on 60-days' prior notice, whereupon Customer may submit to Reseller a claim for a refund of any prepaid subscription fees covering any prepaid subscription fees covering that part of the applicable Subscription Term for such Subscription Service remaining after the effective date of termination.

7.1.3. LIMITATIONS. Notwithstanding the above, ServiceNow will have no obligation or liability for any Claim under Section 7.1.1(a)(i) to the extent arising in whole or in part from: **(a)** any access to or use of any ServiceNow Core Technology not expressly authorized under this Agreement, to the extent the Claim would have been avoided without such unauthorized access or use; **(b)** Customer Data or Customer Technology; or **(c)** access to or use of the ServiceNow Core Technology: **(i)** in violation of Law; **(ii)** after termination under Section 7.1.2(d); **(iii)** as modified to Customer's specifications or by anyone other than ServiceNow or its contractors, if the Claim would have been avoided but for such modifications; or **(iv)** combined with anything not provided by ServiceNow, if the Claim would have been avoided but for such combination.

7.2 CUSTOMER OBLIGATION. Customer will: **(a)** defend ServiceNow and ServiceNow Affiliates, and its and their officers, directors, and employees against any Claim to the extent alleging that Customer Data, Customer Technology, or a modification to any ServiceNow Core Technology made to Customer's specifications or otherwise

made by or on behalf of Customer by any person other than ServiceNow or a person acting at ServiceNow's direction (but only if the Claim would have been avoided by use of the unmodified ServiceNow Core Technology), infringes any patent, copyright, or trademark, misappropriates any third-party trade secret, or violates any third-party privacy rights; and **(b)** pay any settlement amount or any court-ordered award of damages, under the foregoing subsection (a) to the extent arising from such Claim.

7.3 PROCESS. The obligations of ServiceNow and Customer under Sections 7.1 and 7.2 are conditioned on the indemnified party **(a)** notifying the indemnifying party promptly in writing of any actual or threatened Claim, **(b)** the indemnified party giving the indemnifying party sole control of the defense of such Claim and of any related settlement negotiations, and **(c)** the indemnified party cooperating and, at the indemnifying party's reasonable request and expense, assisting in such defense. Neither party will stipulate, acknowledge, or admit fault or liability on the other's part without the other's prior, written consent. The indemnifying party will not publicize any settlement without the indemnified party's prior, written consent. **To the extent the parties perform as required, this Section 7 states each party's entire liability and the other party's exclusive remedy for third-party claims and third-party actions.**

8. LIMITED LIABILITY

Servicenow shall have no liability for any refund that, in accordance with the terms of this Agreement, is to be paid by Reseller. To the extent permitted by Law, each party's total, cumulative liability arising out of or related to this Agreement and the products and services provided under it, whether based on contract, tort (including negligence), or any other legal or equitable theory, will be limited to the amounts paid by Customer for use of the products or provision of the services giving rise to the claim during the 12-month period preceding the first event giving rise to liability. The existence of more than one claim will not enlarge this limit. The foregoing limitation of liability shall not apply to: (a) Customer's obligation to pay for products, services or taxes; (b) a party's obligations in Section 7 (Indemnification); and (c) infringement by a party of the other party's Intellectual Property Rights.

9. EXCLUDED DAMAGES

To the extent permitted by Law, neither ServiceNow nor Customer will be liable to the other or any third party for lost profits (direct or indirect) or loss of use or data or for any incidental, other consequential, punitive, special, or exemplary damages (including damage to business, reputation, or goodwill), or indirect damages of any type however caused, whether by breach of warranty, breach of contract, in tort (including negligence), or any other legal or equitable cause of action, even if such party has been advised of such damages in advance or if such damages were foreseeable. The foregoing exclusions shall not apply to: (a) payments to a third party arising from a party's obligations under Section 7 (Indemnification); and (b) infringement by a party of the other party's Intellectual Property Rights.

10. GROSS NEGLIGENCE; WILLFUL MISCONDUCT

As provided by Law, nothing herein shall be intended to limit a party's liability in an action in tort, separate and distinct from a cause of action for breach of this Agreement, for the party's gross negligence or willful misconduct.

11. TERM AND TERMINATION

11.1 TERMINATION. This Agreement begins on the Effective Date and continues until terminated under its terms. Each party may terminate this Agreement in its entirety: **(a)** on 30 days' prior notice to the other, if at the time of notice there are no Use Authorizations in effect; **(b)** immediately on notice if the other party becomes the subject of a petition in bankruptcy or any proceeding related to its insolvency, receivership, or liquidation, in any jurisdiction, that is not dismissed within 60 days of its commencement or an assignment for the benefit of creditors; or **(c)** immediately on notice if the other party materially breaches this Agreement and does not cure such breach within 30 days after the other party's receipt of notice of the breach. Either party may terminate a Use Authorization or SOW on notice if the other party materially breaches this Agreement or the applicable Use Authorization or SOW for the affected service and does not cure the breach within 30 days after receiving notice of the breach from the non-breaching party. Professional Services are separately ordered from the Subscription Service and are not required for use of the Subscription Service. A breach by a party of its obligations with respect to Professional

Services shall not by itself constitute a breach by that party of its obligations with respect to the Subscription Service even if the services are enumerated in the same Use Authorization.

11.1.1. EFFECT OF TERMINATION OF SUBSCRIPTION SERVICE. On termination or expiration of the Subscription Service, Customer will stop accessing and using, and ServiceNow will stop providing, the Subscription Service and all related rights granted to Customer in this Agreement will terminate immediately, automatically, and without notice. Customer, within 30 days after the effective date of termination by Customer for ServiceNow's breach, submit to Reseller a claim for refund for any prepaid fees paid to Reseller covering that part of the Subscription Term for the affected Subscription Service, if any, remaining after the effective date of termination. Within 30 days after the effective date of termination by ServiceNow for Customer's breach, Customer shall pay all remaining amounts for the Subscription Term applicable to the Subscription Service covering the remainder of the Subscription Term regardless of the due dates specified in an applicable ordering document between Reseller and Customer.

11.2 RETURN OF CUSTOMER DATA. After termination or expiration of this Agreement or the applicable Subscription Service, upon Customer's written request, ServiceNow will provide any Customer Data in the Subscription Service to Customer in ServiceNow's standard database export format at no additional charge. Customer must submit such request to ServiceNow within 45 days after termination or expiration of this Agreement or the Subscription Service. ServiceNow is not obligated to maintain or provide any Customer Data after such 45-day period and will, unless legally prohibited, delete all Customer Data in its systems or otherwise in its possession or under its control, and delete Customer's instances of the Subscription Service.

11.3 SURVIVAL. Sections 2.2 (Restrictions), 4 (Intellectual Property), 5 (Warranties; Disclaimer of Warranties) (solely in accordance with its terms), 6 (Confidential Information) through 10 (Gross Negligence; Willful Misconduct), 11 (Term and Termination) (solely in accordance with its terms), and 12 (General Provisions), together with any other terms required for their construction or enforcement, will survive termination or expiration of this Agreement.

12. GENERAL PROVISIONS

12.1 ASSIGNMENT. Neither party may assign or novate its rights or obligations under this Agreement, by operation of law or otherwise (any of the foregoing, "**Assign**"), without the other party's prior written consent. Notwithstanding the foregoing, on notice and without the other's consent: **(a)** either party may in connection with a merger, reorganization, or sale of all or substantially all of such party's assets or equity, Assign this Agreement in its entirety to such party's successor; and **(b)** ServiceNow may Assign this Agreement in its entirety to any ServiceNow Affiliate. Any attempted or purported Assignment in violation of this Section 12.1 will be null and void. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties, their respective successors, and permitted assigns.

12.2 COMPLIANCE WITH LAWS. ServiceNow will comply with all Laws applicable to its provision under the Agreement of the ServiceNow Products, including those applicable to privacy and security of personal information (including mandatory trans-border data transfers and mandatory data breach notification requirements), but excluding Laws specifically applicable to Customer and its industry not generally applicable to information technology service providers regardless of industry. Customer will comply with all Laws applicable to its use of the ServiceNow Products, including those applicable to collection and processing of Customer Data in ServiceNow systems through the Subscription Service. Customer agrees to provide any required disclosures to and obtain any required consents for the transfer of Customer Data to ServiceNow.

12.3 EXPORT COMPLIANCE. Each party will comply with local and foreign export control Laws, including U.S. export control Laws. Customer acknowledges that the ServiceNow Products are subject to U.S. Export Administration Regulations ("**EAR**") and that Customer will comply with EAR. Without limiting the foregoing, Customer represents and warrants that: **(a)** it is not located in, and will not use any ServiceNow Products from, any country subject to U.S. export restrictions (currently including Cuba, Iran, North Korea, Sudan, Syria, and Crimea Region); **(b)** Customer will not use the ServiceNow Products in the design, development, or production of nuclear, chemical, or biological weapons, or rocket systems, space launch vehicles, sounding rockets, or unmanned air vehicle systems; and **(c)** Customer is not prohibited from participating in U.S. export transactions by any federal agency of the U.S. government. In addition, Customer is responsible for complying with any local Laws that may impact Customer's right to import, export, or use ServiceNow Products or any of them.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

12.4 US GOVERNMENT RIGHTS. ServiceNow software is commercial computer software (as defined in Federal Acquisition Regulation ("**FAR**") 2.101 for civilian agency purchases and Department of Defense ("**DOD**") FAR Supplement ("**DFARS**") 252.227-7014(a)(1) for defense agency purchases) and ServiceNow services are commercial items. If the software is licensed or services acquired by or on behalf of a civilian agency, ServiceNow provides the software, its documentation, and any other technical data subject to this Agreement consistent with FAR 12.212 (Computer Software) and FAR 12.211 (Technical Data). If software is licensed or services acquired by or on behalf of any DOD agency, ServiceNow provides the software, its documentation, and any other technical data subject to this Agreement consistent with DFARS 227.7202-3. If this is a DOD prime contract or DOD subcontract, the DOD agency Customer may acquire additional rights in technical data under DFARS 252.227-7015(b). This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

12.5 NOTICE. Except as otherwise provided in this Agreement, all notices will be in writing and deemed given on: **(a)** personal delivery; **(b)** when received by the addressee if sent by a recognized overnight courier (receipt requested); **(c)** the third business day after mailing; or **(d)** the first business day after sending by email with confirmation of receipt, except that email will not be sufficient for notices regarding a Claim or alleged breach. Notices will be sent as set forth on the first page of this Agreement or as subsequently updated in writing.

12.6 FORCE MAJEURE. ServiceNow is not, and may not be construed to be, in breach of this Agreement for any failure or delay in fulfilling or performing the Subscription Service or any Professional Services, when and to the extent such failure or delay is caused by or results from acts beyond ServiceNow's reasonable control, including: strikes, lock-outs, or other industrial disputes; trespass, sabotage, theft or other criminal acts export bans, sanctions, war, terrorism, riot, civil unrest, or government action; failure of Internet connectivity or backbone or other telecommunications failures, in each case outside of ServiceNow's local network; breakdown of plant or machinery; nuclear, chemical, or biological contamination; fire, flood, natural disaster, extreme adverse weather, or other acts of God (each a "**Force Majeure Event**"). ServiceNow will use reasonable efforts to mitigate the effects of such Force Majeure Event.

12.7 HIGH RISK ACTIVITY. The ServiceNow Products are not designed for any purpose requiring fail-safe performance, including stock trading, financial transaction processing, operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, weapons systems, or other management or operation of hazardous facilities or applications for which failure could result in death, personal injury, or severe physical, property, or environmental damage (each, a "**High Risk Activity**"). ServiceNow, its licensors, and suppliers expressly disclaim all warranties of fitness for any such use.

12.8 EXECUTION. This Agreement may be executed in counterparts, by electronic means to accurately send images, such as via email, or by electronic signature service. Neither party will contest the Agreement's validity solely because a signature was faxed or sent through other permitted electronic means. Each party will deliver to the other an original executed copy of the Agreement promptly after execution.

12.9 WAIVER AND AMENDMENT. Failure by a party to enforce any part of this Agreement will not be deemed a waiver of future enforcement of that or any other provision. A waiver of any right is effective only if in a writing signed by an authorized representative of the waiving party. Any modification of this Agreement must be in writing and signed by authorized representatives of both parties.

12.10 SEVERABILITY. If any term of this Agreement is held invalid, unenforceable, or void by a court of competent jurisdiction, such term will be enforced to the maximum extent permissible, such holding will not affect the remaining terms, and the invalid, unenforceable, or void term will be deemed amended or replaced by a valid, legal, and enforceable term that matches the intent of the original language as closely as possible.

12.11 RELATIONSHIP. The parties are independent contractors. Nothing in this Agreement will be construed to create a partnership, joint venture, agency, or other relationship. Neither party has any right or authority to assume or create any obligation of any kind, express or implied, in the other party's name or on its behalf. No third-party is a third-party beneficiary of, or liable under, this Agreement, and no third-party is responsible for any obligations or liability arising out of Customer's use of the ServiceNow Core Technology.

12.12 GOVERNING LAW; JURISDICTION AND VENUE. This Agreement will be governed by the Laws of the State of California, without regard to its conflict of laws principles. The parties irrevocably consent to the exclusive jurisdiction of, and venue in, any federal or state court of competent jurisdiction located in Santa Clara County, California, for the purposes of adjudicating any dispute arising out of or related to this Agreement. Each

servicenow

SUBSCRIPTION SERVICE AGREEMENT

party expressly consents to service of process by registered mail. To the extent permitted by Law, choice of law rules and the United Nations Convention on Contracts for the International Sale of Goods will not apply. Notwithstanding the foregoing, either party may at any time seek and obtain appropriate legal or equitable relief in any court of competent jurisdiction for claims regarding such party's Intellectual Property Rights.

12.13 EQUITABLE REMEDIES. The receiving party's disclosure of Confidential Information except as provided in this Agreement, or a party's infringement or misappropriation of the other party's Intellectual Property Rights may result in irreparable injury for which a remedy in money damages may be inadequate. In the event of such actual or threatened disclosure, infringement or misappropriation, disclosing party may be entitled to seek an injunction to prevent the breach or threatened breach without the necessity of proving irreparable injury or the inadequacy of money damages, in addition to remedies otherwise available to disclosing party at law or in equity.

12.14 CONSTRUCTION. ServiceNow is obligated to provide ServiceNow Products only in the English language, unless otherwise agreed in writing. The parties have expressly requested that this Agreement and all related documents be drafted in English. *Les parties confirment avoir expressément exigé que le présent contrat et les documents de ServiceNow qui y sont attachés soient rédigés en anglais.* Section headings are for convenience only and are not to be used in interpreting this Agreement. This Agreement has been negotiated by the parties and their respective counsel and will be interpreted fairly in accordance with its terms and without any strict construction in favor of or against either party. Lists of examples following "including", "e.g.", "such as", or "for example" are interpreted to include "without limitation", unless qualified by words such as "only" or "solely." Unless stated or context requires otherwise: **(a)** all internal references are to this Agreement, its parties, and its Exhibits; **(b)** "days" means calendar days; **(c)** "may" means that the applicable party has a right, but not a concomitant duty; **(d)** all monetary amounts are expressed and, if applicable, payable, in U.S. dollars; **(e)** "current" or "currently" means "as of the Effective Date" but "then-current" means the present time when the applicable right is exercised or performance rendered or measured; **(f)** the word "or" will be deemed to be an inclusive "or"; **(g)** URLs are understood to also refer to successor URLs, URLs for localized content, and information or resources linked from within the websites at such URLs; **(h)** a writing is "signed" when it has been hand-signed (i.e., with a pen) or electronically signed using an electronic signature service by duly authorized representatives of both parties; **(i)** a party's choices, elections, and determinations under this Agreement are in its sole discretion; **(j)** the singular includes the plural and vice versa; **(k)** a reference to a document includes any amendment, replacement, or novation of it; and **(m)** a reference to a thing includes a part of that thing (i.e., is interpreted to include "in whole or in part").

12.15 ENTIRETY. This Agreement (together with the Use Authorizations, Product Overviews, SOWs, and Service Descriptions, all of which are also deemed incorporated by this reference) is the parties' entire agreement regarding its subject matter and supersedes all prior or contemporaneous oral or written agreements, representations, understandings, undertakings, negotiations, letters of intent, and proposals, with respect to such subjects. The terms of this Agreement apply to the exclusion of any other terms Customer seeks to impose or incorporate, or that may be implied by trade, custom, practice, or course of dealing. Customer acknowledges it has not relied on any statement, promise, or representation made or given by or on behalf of ServiceNow that is not expressly stated in this Agreement. Customer's orders are not contingent, and Customer has not relied, on the delivery of any future functionality regardless of any verbal or written communication about ServiceNow's possible future plans.

12.16 COUNTRY SPECIFIC PROVISIONS. The following country-specific provisions will replace or supplement the equivalent provisions of the Agreement as set forth below depending on the domicile of Customer.

AUSTRALIA

The following language shall be added as a new Section 5.4 of the General Terms and Conditions:

> COMPLIANCE WITH CONSUMER LAWS. **To the extent, if any, that the terms and conditions of the Competition and Consumer Act 2010 (Cth), including the Australian Consumer Law, or other statutory Law prevents ServiceNow from excluding certain liability as set forth in the Agreement, such liability will be limited to the extent permitted by such Law to one or more of the following: (a) in respect of a supply of services, to: (i) the supplying of the services again, or (ii) the payment of the cost of having the services supplied again; and (b) in respect of a supply of goods, to: (i) the replacement of the**

servicenow

SUBSCRIPTION SERVICE AGREEMENT

goods or the supply of equivalent goods, (ii) the repair of the goods, (iii) the payment of the cost of replacing the goods or of acquiring equivalent goods, or (iv) the payment of the cost of having the goods repaired. Notwithstanding any other provision of this Agreement or any Order Form to the contrary, nothing therein will derogate from any requirement to provide a refund under the Australian Consumer Law. If Customer is acquiring goods or services as a "consumer" for the purposes of the Australian Consumer Law, the benefits given any warranties that are a "warranty against defects" (as such term is defined in the Australian Consumer Law) are in addition to any other rights and remedies available to Customer under a law in relation to the goods or services to which such warranty relates and, in such case, "Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure."

The following language shall replace section 12.12 of the General Terms and Conditions:

GOVERNING LAW; JURISDICTION AND VENUE. This Agreement shall be governed by the laws of the state of New South Wales, Australia without regard to its conflict of laws principles. The parties hereby irrevocably consent to the exclusive jurisdiction of, and venue in, any federal or state court of competent jurisdiction located in New South Wales, Australia for the purposes of adjudicating any dispute arising out of this Agreement. Each party hereto expressly consents to service of process by registered mail. To the extent permitted by law, choice of law rules and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. Notwithstanding the foregoing, either party may at any time seek and obtain appropriate legal or equitable relief in any court of competent jurisdiction for claims regarding such party's intellectual property rights.

///
///
///

Remainder of page intentionally left blank

servicenow

SUBSCRIPTION SERVICE AGREEMENT

EXHIBIT A.1 - SUBSCRIPTION SERVICE GUIDE

1. SUPPORT

ServiceNow will provide support for the Subscription Service as set forth in the ***Customer Support Policy*** attached to this Subscription Service Guide as Exhibit A.2 and incorporated herein by reference. The Customer Support Policy may be updated periodically.

2. UPGRADES AND UPDATES

ServiceNow will provide upgrades and updates to the Subscription Service as described in Exhibit A.3 ***Upgrades and Updates*** attached to this Subscription Service Guide and incorporated herein by reference. The Upgrade and Update exhibit may be updated periodically.

3. DATA PROCESSING ADDENDUM

The parties' agreement with respect to the processing of personal information submitted to the Subscription Service is described in the ***Data Processing Addendum*** attached to this Subscription Service Guide as Exhibit A.4 and incorporated herein by reference. The Data Processing Addendum may be updated periodically.

4. DATA SECURITY GUIDE

ServiceNow will implement and maintain security procedures and practices appropriate to information technology service providers designed to protect Customer Data from unauthorized access, destruction, use, modification, or disclosure, as described in the ***Data Security Guide*** attached to this Subscription Service Guide as Exhibit A.5 and incorporated herein by reference. The Data Security Guide may be updated periodically.

5. INSURANCE

ServiceNow agrees to maintain in effect during the Subscription Term, at ServiceNow's expense, the following minimum insurance coverage:

5.1 Workers' Compensation Insurance, in accordance with applicable statutory, federal, and other legal requirements;

5.2 Employers' Liability Insurance covering ServiceNow's employees in an amount of not less than $1,000,000 for bodily injury by accident and $1,000,000 each employee for bodily injury by disease;

5.3 Commercial General Liability Insurance written on an occurrence form and including coverage for bodily injury, property damage, products and completed operations, personal injury, and advertising injury arising out of the products or services provided by ServiceNow under this Agreement, with minimum limits of $1,000,000 per occurrence/$2,000,000 aggregate;

5.4 Commercial Automobile Liability Insurance providing coverage for hired and non-owned automobiles used in connection with this Agreement in an amount of not less than $1,000,000 per accident, combined single limit for bodily injury and property damage;

5.5 Combined Technology Errors' & Omissions Policy with a $5,000,000 per claim limit, including: **(a)** Professional Liability Insurance providing coverage for the services and software in this Agreement (which coverage will be maintained for at least two years after termination of this Agreement); and **(b)** Privacy, Security, and Media Liability Insurance providing liability coverage for unauthorized access or disclosure, security breaches, and system attacks, as well as infringements of copyright and trademark that might result from this Agreement; and

5.6 Excess Liability over Employers' Liability, Commercial General Liability, and Commercial Automobile Liability, with a $5,000,000 aggregate limit.

For the purpose of this Section 5, a "claim" means a written demand for money or a civil proceeding which is commenced by service of a complaint or similar pleading.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

6. AVAILABILITY SERVICE LEVEL

6.1 DEFINITIONS.

6.1.1. "**Available**" means that the Subscription Service can be accessed by authorized users.

6.1.2. "**Excused Downtime**" means: **(a)** Maintenance Time of up to two hours per month; and **(b)** any time the Subscription Service is not Available due to circumstances beyond ServiceNow's control, including modifications of the Subscription Service by any person other than ServiceNow or a person acting at ServiceNow's direction, a Force Majeure Event, general Internet outages, failure of Customer's infrastructure or connectivity (including direct connectivity and virtual private network ("**VPN**") connectivity to the Subscription Service), computer and telecommunications failures and delays, and network intrusions or denial-of-service or other criminal attacks.

6.1.3. "**Infrastructure Modification**" means any repairs, maintenance, improvements, or changes to the cloud infrastructure used by ServiceNow to operate and deliver the Subscription Service.

6.1.4. "**Maintenance Time**" means the time the Subscription Service is not Available due to an Infrastructure Modification, Upgrade, and Update.

6.1.5. "**Availability SLA**" means that the production instances of the Subscription Service will be Available at least 99.8% of the time during a calendar month, excluding Excused Downtime.

6.2 AVAILABILITY. If Customer's production instances of the Subscription Service fall below the Availability SLA during a calendar month, Customer's exclusive remedy for failure of the Subscription Service to meet the Availability SLA is to request that either: **(a)** the affected Subscription Term be extended for the number of minutes the Subscription Service was not Available in the month in accordance with the Availability SLA; or **(b)** ServiceNow issue a service credit to Customer for the dollar value of the number of minutes the Subscription Service was not Available in the month in accordance with the Availability SLA (determined at the deemed per-minute rate ServiceNow charges to Customer for Customer's use of the affected Subscription Service), which Customer may request ServiceNow apply to the next invoice for subscription fees.

6.3 REQUESTS. Customer must request all service credits or extensions in writing to ServiceNow within 30 days of the end of the month in which the Availability SLA was not met, identifying the support requests relating to the period Customer's production instances of the Subscription Service was not Available. The total amount of service credits for any month may not exceed the subscription fee for the affected Subscription Service for that month and has no cash value. ServiceNow may delay issuing service credits until such amounts reach $1,000 USD or equivalent currency specified in the applicable Order Form.

6.4 NOTICE. ServiceNow will give Customer 10 days' prior notice of an Infrastructure Modification if ServiceNow, in its reasonable judgment, believes that the Infrastructure Modification will impact Customer's use of its production instances of the Subscription Service, unless, in the reasonable judgment of ServiceNow, the Infrastructure Modification is necessary to: **(a)** maintain the availability, security, or performance of the Subscription Service; **(b)** comply with Law; or **(c)** avoid infringement or misappropriation of third-party Intellectual Property Rights.

///
///
///
Remainder of page intentionally left blank

servicenow

SUBSCRIPTION SERVICE AGREEMENT

EXHIBIT A.2 - CUSTOMER SUPPORT POLICY

This Customer Support Policy governs the support that ServiceNow will provide for its Subscription Service ("**Customer Support**").

1. SCOPE

The purpose of Customer Support is to resolve defects that cause a nonconformity in the Subscription Service as compared to the Product Overview. A resolution to a defect may consist of a fix, workaround, or other relief, as ServiceNow deems reasonable. Customer Support does not include performing the following services:

- implementation services;
- configuration services;
- integration services;
- customization services or other custom software development;
- training; or
- assistance with administrative functions.

Customer Support is not required to provide resolutions for immaterial defects or defects due to modifications of the Subscription Service made by any person other than ServiceNow or a person acting at ServiceNow's direction, or defects on any instance of the Subscription Service not in conformance with Exhibit A.3 - Upgrades and Updates.

2. BUSINESS HOURS

Customer Support is available 24 hours a day, 7 days a week, including all holidays.

3. ACCESS CONTACTS

ServiceNow's Customer Support portal ("**Support Portal**") is located at https://hi.service-now.com/. Customer may get login access to the Support Portal by contacting its ServiceNow administrator.

ServiceNow's Customer Support may be reached by phone using one of the numbers at http://servicenow.com/support/contact-support.html.

4. INCIDENT PRIORITY

Incident priority for a defect is determined using the guidelines below.

Priority	Definition
P1	Any defect that causes an instance not to be Available.
P2	Any defect that causes a critical function to fail.
P3	Any defect that significantly impedes work or progress.
P4	Any defect that does not significantly impede work or progress.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

5. RESPONSE TIMES AND LEVEL OF EFFORT

Customer may submit an incident with ServiceNow via the Support Portal or phone. Response times are not affected by the manner of contact. All support requests are tracked in the Support Portal and can be viewed by Customer's authorized contacts. ServiceNow will use reasonable efforts to meet the target response times and target level of effort stated in the table below.

Priority	Target Response Times	Target Level of Effort
P1	30 minutes	Continuously, 24 hours per day, 7 days per week
P2	2 hours	Continuously, but not necessarily 24 hours per day, 7 days per week
P3	1 business day	As appropriate during normal business hours
P4	N/A	Varies

6. CUSTOMER RESPONSIBILITIES

Customer's obligations with respect to Customer Support are as follows:

6.1 Customer will receive from ServiceNow communications via email, phone, or through the Support Portal regarding the Subscription Service.

6.2 Customer will appoint no more than 10 contacts ("**Customer Authorized Contacts**") to engage Customer Support for questions and technical issues.

6.2.1. Customer must maintain the following Customer Authorized Contacts:

- Primary Business Contact;
- Secondary Business Contact;
- Technical Contact;
- Support Contact;
- Primary Customer Administrator; and
- Security Contact.

6.2.2. Customer will maintain current information for all Customer Authorized Contacts in the Support Portal.

6.2.3. Only Customer Authorized Contacts will contact Customer Support.

6.2.4. Customer will train all Customer Authorized Contacts on the use and administration of the Subscription Service.

6.3 Customer will cooperate to enable ServiceNow to deliver the Subscription Service and Customer Support.

6.4 Customer is solely responsible for the use of the Subscription Service by its users.

///
///
///

Remainder of page intentionally left blank

servicenow

SUBSCRIPTION SERVICE AGREEMENT

EXHIBIT A.3 - UPGRADES AND UPDATES

7. DEFINITIONS

7.1 "**Upgrades**" are ServiceNow's releases of the Subscription Service for enhancements or new features (including a new Release Family) applied by ServiceNow to Customer's instances of the Subscription Service at no additional fee during the Subscription Term.

7.2 "**Updates**" are ServiceNow's releases (including patches and hotfixes) of the Subscription Service applied by ServiceNow to Customer's instances of the Subscription Service at no additional fee during the Subscription Term that provide problem fixes, but do not generally include new functionality, and are released as needed.

7.3 "**Release Family**" is an Upgrade that is a complete solution with new features or enhancements, including previously released Updates if applicable to the features included in the Upgrade. For example, ServiceNow's "Geneva" Upgrade established the "Geneva Release Family", and ServiceNow's "Helsinki" Upgrade established the "Helsinki Release Family".

7.4 "**Critical Upgrade**" is an Upgrade that in ServiceNow's reasonable judgment is critical to maintaining the availability, security or performance of the Subscription Service; comply with applicable laws or to avoid infringement or misappropriation of a third-party Intellectual Property Right.

7.5 "**Critical Update**" is an Update that in ServiceNow's reasonable judgment is critical to maintaining the availability, security or performance of the Subscription Service; comply with applicable laws or to avoid infringement or misappropriation of a third-party Intellectual Property Right.

7.6 "**Supported Release Family**" at a particular time means the then-current Release Family and the prior 2 Release Families.

8. UPGRADES AND UPDATES

ServiceNow shall determine, in its sole discretion: **(a)** whether and when to develop, release and apply any Update or Upgrade to Customer's instances of the Subscription Service; and **(b)** whether a particular release is an Update, Upgrade or new service offering that is available separately for purchase.

9. NOTICE

ServiceNow shall: **(a)** give Customer 30 days' notice of any Upgrade to the Subscription Service; and **(b)** use reasonable efforts to give Customer 10 days' notice of any Update to the Subscription Service. Notwithstanding the foregoing, ServiceNow may provide Customer with shorter notice or no notice before the application of a Critical Upgrade or a Critical Update.

10. SUPPORTED AND NON-SUPPORTED RELEASE FAMILIES

Customer acknowledges that the current Release Family is the version of the Subscription Service containing the most current features, availability, performance and security. Within a Supported Release Family, the most recent Update is the version of the Subscription Service for that Release Family that contains the most current problem fixes, availability, performance and security. A Customer using a Supported Release Family may be required to apply a Critical Update within the Supported Release Family. A Customer that has not Upgraded to a Supported Release Family may experience defects, for which Customer hereby agrees that ServiceNow is not responsible, including without limitation those that affect the features, availability, performance and security of the Subscription Service, that are fixed in the most current version of the Subscription Service. A Customer who is not using a Supported Release Family may be required to apply an Upgrade to a Supported Release Family.

///
///
///

Remainder of page intentionally left blank

servicenow

SUBSCRIPTION SERVICE AGREEMENT

EXHIBIT A.4 - DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") is deemed to include Sections 1 through 9 below, including the attached Appendix 1, and the Data Security Guide, all of which are expressly deemed incorporated in the Agreement by this reference.

In the event of any conflict between the terms of this DPA and the terms of the Agreement with respect to the subject matter herein, this DPA shall control. Any data processing agreements that may already exist between parties as well as any earlier version of the Data Security Guide to which the parties may have agreed are superseded and replaced by this DPA in their entirety. All capitalized terms not defined in this DPA will have the meaning given to them in other parts of the Agreement.

1. DEFINITIONS

1.1 "**Affiliates**" means any person or entity directly or indirectly Controlling, Controlled by or under common Control with a party to the Agreement, where "**Control**" means the legal power to direct or cause the direction of the general management of the company, partnership, or other legal entity.

1.2 "**Agreement**" means the Order Form or Use Authorization or other signed ordering document, as applicable, between ServiceNow and Customer and the signed master agreement (if any) for the purchase of the Subscription Service.

1.3 "**Data Controller**" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data. For purposes of this DPA, Data Controller is Customer and, where applicable, its Affiliates either permitted by Customer to submit Personal Data to the Subscription Service or whose Personal Data is Processed in the Subscription Service.

1.4 "**Data Processor**" means the natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Data Controller. For purposes of this DPA, Data Processor is the ServiceNow entity that is a party to the Agreement.

1.5 "**Data Protection Laws**" means all applicable laws and regulations regarding the Processing of Personal Data and includes GDPR.

1.6 "**Data Subject**" means an identified or identifiable natural person.

1.7 "**GDPR**" means the European Union's General Data Protection Regulation (2016/679).

1.8 "**Instructions**" means Data Controller's documented data Processing instructions issued to Data Processor in compliance with this DPA.

1.9 "**Personal Data**" means any information relating to a Data Subject uploaded by or for Customer or Customer's agents, employees, or contractors to the Subscription Service as Customer Data.

1.10 "**Process**" or "**Processing**" means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.11 "**Professional Services**" means any consulting or development services provided by or on behalf of ServiceNow pursuant to an agreed Statement of Work or Service Description described or referenced in a signed ordering document.

1.12 "**Sub-Processor**" means any legal person or entity engaged in the Processing of Personal Data by Data Processor. For the avoidance of doubt, ServiceNow's colocation datacenter facilities are not Sub-Processors under this DPA.

1.13 "**Subscription Service**" means the ServiceNow software-as-a-service offering ordered by Customer under a Use Authorization, Use Authorization or other signed ordering document between ServiceNow and Customer.

1.14 "**Subscription Term**" means the term of authorized use of the Subscription Service as set forth in the Order Form, Use Authorization, or other ordering document signed by Customer and ServiceNow.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

2. SCOPE OF THE PROCESSING

2.1 COMMISSIONED PROCESSOR. Data Controller appoints Data Processor to Process Personal Data on behalf of Data Controller to the extent necessary to provide the Subscription Service described in the Agreement and in accordance with the Instructions.

2.2 INSTRUCTIONS. The Agreement constitutes Data Controller's written Instructions to Data Processor for Processing of Personal Data. Data Controller may issue additional or alternate Instructions provided that such Instructions are: (a) consistent with the purpose and the scope of the Agreement; and (b) confirmed in writing by Data Controller. For the avoidance of doubt, Data Controller shall not use additional or alternate Instructions to alter the scope of the Agreement. Data Controller is responsible for ensuring its Instructions to Data Processor comply with Data Protection Laws.

2.3 NATURE, SCOPE AND PURPOSE OF THE PROCESSING. Data Processor shall only Process Personal Data in accordance with Data Controller's Instructions and to the extent necessary for providing the Subscription Service and the Professional Services, each as described in the Agreement. Data Controller acknowledges that all Personal Data it instructs Data Processor to Process for the purpose of providing the Professional Services must be limited to the Customer Data Processed within the Subscription Service.

2.4 CATEGORIES OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS. Data Controller may submit Personal Data to the Subscription Service as Customer Data, the extent of which is determined and controlled by Data Controller in its sole discretion and is further described in Appendix 1.

3. DATA CONTROLLER

3.1 COMPLIANCE WITH DATA PROTECTION LAWS. Data Controller shall comply with all of its obligations under Data Protection Laws when Processing Personal Data.

3.2 SECURITY RISK ASSESSMENT. Data Controller agrees that in accordance with Data Protection Laws and before submitting any Personal Data to the Subscription Service, Data Controller will perform an appropriate risk assessment to determine whether the security measures within the Subscription Service provide an adequate level of security, taking into account the nature, scope, context and purposes of the processing, the risks associated with the Personal Data and the applicable Data Protection Laws. Data Processor shall provide Data Controller reasonable assistance by providing Data Controller with information requested by Data Controller to conduct Data Controller's security risk assessment. Data Controller is solely responsible for determining the adequacy of the security measures within the Subscription Service in relation to the Personal Data Processed. As further described in Section 7.1 (Product Capabilities) of the Data Security Guide, the Subscription Service includes, without limitation, column level encryption functionality and role-based access control, which Data Controller may use in its sole discretion to ensure a level of security appropriate to the risk of the Personal Data. For clarity, Data Controller may influence the scope and the manner of Processing of its Personal Data by its own implementation, configuration (i.e., different types of encryption) and use of the Subscription Service, including any other products or services offered by ServiceNow and third-party integrations.

3.3 CUSTOMER'S AFFILIATES. The obligations of Data Processor set forth herein will extend to Customer's Data Controller Affiliates to which Customer provides access to the Subscription Service or whose Personal Data is Processed within the Subscription Service, subject to the following conditions:

3.3.1. COMPLIANCE. Customer shall at all times be liable for its Affiliates' compliance with this DPA and all acts and omissions by a Data Controller Affiliate are considered acts and omissions of Customer; and

3.3.2. CLAIMS. Customer's Data Controller Affiliates will not bring a claim directly against Data Processor. In the event a Data Controller Affiliate wishes to assert a valid legal action, suit, claim or proceeding against Data Processor (a "**Data Controller Affiliate Claim**"): (i) Customer must bring such Data Controller Affiliate Claim directly against Data Processor on behalf of such Data Controller Affiliate, unless Data Protection Laws require that Data Controller Affiliate be party to such Data Controller Affiliate Claim; and (ii) all Data Controller Affiliate Claims will be considered claims made by Customer and are at all times subject to any aggregate limitation of liability set forth in the Agreement.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

3.3.3. DATA CONTROLLER AFFILIATE ORDERING. If a Data Controller Affiliate purchased a separate instance of the Subscription Service under the terms of the signed master agreement between ServiceNow and Customer, then such Data Controller Affiliate will be deemed a party to this DPA and shall be treated as Customer under the terms of this DPA.

3.4 COMMUNICATION. Unless otherwise provided in this DPA, all requests, notices, cooperation, and communication, including Instructions issued or required under this DPA (collectively, "**Communication**"), must be in writing and between Customer and ServiceNow only and Customer shall inform the applicable Data Controller Affiliate of any Communication from ServiceNow pursuant to this DPA. Customer shall be solely responsible for ensuring that any Communications (including Instructions) it provides to ServiceNow relating to Personal Data for which a Customer Affiliate is Data Controller reflect the relevant Customer Affiliate's intentions.

4. DATA PROCESSOR

4.1 DATA CONTROLLER'S INSTRUCTIONS. Data Processor will have no liability for any harm or damages resulting from Data Processor's compliance with Instructions received from Data Controller. Where Data Processor believes that compliance with Data Controller's Instructions could result in a violation of Data Protection Laws or is not in the ordinary course of Data Processor's obligations in operating the Subscription Service or delivering Professional Services, Data Processor shall promptly notify Data Controller thereof. Data Controller acknowledges that Data Processor is reliant on Data Controller's representations regarding the extent to which Data Controller is entitled to Process Personal Data.

4.2 DATA PROCESSOR PERSONNEL. Access to Personal Data by Data Processor will be limited to personnel who require such access to perform Data Processor's obligations under the Agreement and who are bound by obligations to maintain the confidentiality of such Personal Data at least as protective as those set forth herein and in the Agreement.

4.3 DATA SECURITY MEASURES. Without prejudice to Data Controller's security risk assessment obligations under Section 3.2 (Security Risk Assessment) above, Data Processor shall maintain appropriate technical and organizational safeguards to protect the security, confidentiality, and integrity of Customer Data, including any Personal Data contained therein, as described in Section 2 (Physical, Technical, and Administrative Security Measures) of the Data Security Guide. Such measures are designed to protect Customer Data from loss, alteration, unauthorized access, acquisition, use, disclosure, or accidental or unlawful destruction, and include:

4.3.1. SERVICE ACCESS CONTROL. The Subscription Service provides user and role-based access controls. Data Controller is responsible for configuring such access controls within its instance.

4.3.2. LOGGING AND MONITORING. The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.

4.3.3. DATA SEPARATION. Customer Data shall be maintained within a logical single-tenant architecture on multi-tenant cloud infrastructure that is logically and physically separate from ServiceNow's corporate infrastructure.

4.3.4. SERVICE CONTINUITY. The production database servers are replicated in near real time to a mirrored data center in a different geographic region.

4.3.5. TESTING. Data Processor regularly tests, assess and evaluates the effectiveness of its information security program and may periodically review and update such program to address new and evolving security technologies, changes to industry standard practices, and changing security threats.

4.4 DELETION OF PERSONAL DATA. Upon termination or expiration of the Agreement, Data Processor shall return and delete Customer Data, including Personal Data contained therein, as described in the Agreement.

4.5 DATA CENTERS. Data Processor will host Data Controller's instances of the Subscription Service in data centers located in the geographic regions specified on the Order Form, Use Authorization, or other signed ordering document between ServiceNow and Customer.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

4.6 DATA PROTECTION IMPACT ASSESSMENTS (DPIA). Data Processor will, on request, provide Data Controller with reasonable information required to fulfill Data Controller's obligations under GDPR to carry out data protection impact assessments, if any, for Processing of Personal Data within the Subscription Service.

4.7 PRIOR CONSULTATION. Data Processor shall provide reasonable assistance (at Data Controller's expense) in connection with any prior consultation Data Controller is required to undertake with a supervisory authority under Data Protection Laws with respect to Processing of Personal Data in the Subscription Service.

4.8 DATA PROCESSOR ASSISTANCE. Data Processor will assist Data Controller in ensuring compliance with Data Controller's obligations pursuant to Articles 32 to 36 of GDPR taking into account the nature of Processing by providing Data Controller with reasonable information requested pursuant to the terms of this DPA, including information required to conduct Data Controller's security risk assessment and respond to Data Subject Requests (defined below). For clarity, Data Controller is solely responsible for carrying out its obligations under GDPR and this DPA. Data Processor shall not undertake any task that can be performed by Data Controller.

4.9 DATA PROTECTION CONTACT. ServiceNow and its Sub-Processor Affiliates (defined below) will maintain a dedicated data protection team to respond to data protection inquiries throughout the duration of this DPA and can be contacted at privacy@servicenow.com.

5. REQUESTS MADE FROM DATA SUBJECTS AND AUTHORITIES

5.1 REQUESTS FROM DATA SUBJECTS. During the Subscription Term, Data Processor shall provide Data Controller with the ability to access, correct, rectify, erase, or block Personal Data, or to transfer or port such Personal Data, within the Subscription Service, as may be required under Data Protection Laws (collectively, "**Data Subject Requests**").

5.2 RESPONSES. Data Controller will be solely responsible for responding to any Data Subject Requests, provided that Data Processor shall reasonably cooperate with the Data Controller to respond to Data Subject Requests to the extent Data Controller is unable to fulfill such Data Subject Requests using the functionality in the Subscription Service. Data Processor will instruct the Data Subject to contact the Customer in the event Data Processor receives a Data Subject Request directly.

5.3 REQUESTS FROM AUTHORITIES. In the case of a notice, audit, inquiry, or investigation by a government body, data protection authority, or law enforcement agency regarding the Processing of Personal Data, Data Processor shall promptly notify Data Controller unless prohibited by applicable law. Data Controller shall keep records of the Personal Data Processed by Data Processor and shall cooperate and provide all necessary information to Data Processor in the event Data Processor is required to produce such information to a data protection authority.

5.4 COOPERATION WITH SUPERVISORY AUTHORITIES. In accordance with Data Protection Laws, Data Controller and Data Processor shall cooperate, on request, with a supervisory authority in the performance of such supervisory authority's task.

6. BREACH NOTIFICATION

6.1 NOTIFICATION. Data Processor will report to Data Controller any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data ("**Breach**") that it becomes aware of without undue delay following determination by ServiceNow that a Breach has occurred.

6.2 REPORT. The initial report will be made to Data Controller's security or privacy contact(s) designated in ServiceNow's customer support portal (or if no such contact(s) are designated, to the primary contact designated by Customer). As information is collected or otherwise becomes available, Data Processor shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Data Controller to notify relevant parties, including affected Data Subjects, government agencies and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the Data Processor contact from whom additional information may be obtained. Data Processor shall inform Customer of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

6.3 DATA CONTROLLER OBLIGATIONS. Data Controller will cooperate with Data Processor in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, including any Breaches, identify its root cause(s), and prevent a recurrence. Data Controller is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.

7. CUSTOMER MONITORING RIGHTS

7.1 REMOTE SELF-ASSESSMENTS. Data Processor shall enable remote self-serve assessments of its Security Program (as defined in the Data Security Guide) by granting Data Controller, at all times and at no additional costs, access to the Data Processor self-access documentation portal ("**ServiceNow CORE**"). The information available on ServiceNow CORE will include documentation evidencing Data Processor's policies, procedures and security measures, as well as copies of the certifications and attestations listed in Section 7.2 (Audit) below.

7.2 AUDIT. No more than once per year and upon written request by Data Controller, Customer shall have the right directly or through its representative(s) (provided however, that such representative(s) shall enter into written obligations of confidentiality directly with Data Processor), to access all reasonable and industry recognized documentation evidencing Data Processor's policies and procedures governing the security of Customer Data ("**Audit**"). Such Audit shall include a written summary report of any assessment performed by an independent third-party of Data Processor's information security management system supporting the Subscription Service against the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent or successor standards). Data Processor reserves the right to refuse to provide Customer (or its representatives) with any information which would pose a security risk to Data Processor or its customers, or which Data Processor is prohibited to provide or disclose under applicable law or contractual obligation.

7.3 OUTPUT. Upon completion of the Audit, Data Processor and Customer may schedule a mutually convenient time to discuss the output of the Audit. Data Processor may in its sole discretion, consistent with industry and Data Processor's standards and practices, make commercially reasonable efforts to implement Customer's suggested improvements noted in the Audit to improve Data Processor's Security Program. The Audit and the results derived therefrom are Confidential Information of Data Processor.

7.4 DATA CONTROLLER EXPENSES. Any expenses incurred by Data Controller in connection with the Audit shall be borne exclusively by Data Controller.

8. SUB-PROCESSORS

8.1 USE OF SUB-PROCESSORS. Data Controller authorizes Data Processor to engage Sub-Processors appointed in accordance with this Section 8 to support the provision of the Subscription Service and to deliver Professional Services as described in the Agreement.

8.1.1. SERVICENOW AFFILIATES. As of the Effective Date, Data Processor engages, as applicable, the following ServiceNow Affiliates as Sub-Processors: ServiceNow, Inc. (USA), ServiceNow Nederland B.V. (the Netherlands), ServiceNow Australia Pty Ltd (Australia), ServiceNow Software Development India Private Limited (India), and ServiceNow UK Ltd. (United Kingdom) (collectively, "**Sub-Processor Affiliates**"). Data Processor will notify Data Controller of changes regarding such Sub-Processor Affiliates through Data Processor's customer support portal (or other mechanism used to notify its general customer base). Each Sub-Processor Affiliate shall comply with the obligations of the Agreement in the Processing of the Personal Data.

8.1.2. NEW SUB-PROCESSORS. Prior to Data Processor or a Data Processor Affiliate engaging a Sub-Processor, Data Processor shall: **(a)** notify Data Controller by email to Customer's designated contact(s) or by notification within the customer support portal (or other mechanism used to notify its customer base); and **(b)** ensure that such Sub-Processor has entered into a written agreement with Data Processor (or the relevant Data Processor Affiliate) requiring that the Sub-Processor abide by terms no less protective than those provided in this DPA. Upon written request by Data Controller, Data Processor shall make a summary of the data processing terms available to Data Controller. Data Controller may request in writing reasonable additional information with respect to Sub-Processor's ability to perform the relevant Processing activities in accordance with this DPA.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

8.2 RIGHT TO OBJECT. Data Controller may object to Data Processor's proposed use of a new Sub-Processor by notifying Data Processor within 10 days after receipt of Data Processor's notice if Data Controller reasonably determines that such Sub-Processor is unable to Process Personal Data in accordance with the terms of this DPA ("**Controller Objection Notice**"). Data Processor shall notify Data Controller within 30 days from receipt of the Controller Objection Notice if Data Processor intends to provide the applicable Professional Service or Subscription Service with the use of the Sub-Processor at issue, and Customer may terminate the applicable Order Form(s), Use Authorization(s) or other signed ordering document between ServiceNow and Customer with respect to the Professional Service or Subscription Service that require use of the Sub-Processor at issue upon written notice to ServiceNow within 45 days of the date of Controller Objection Notice and, as Customer's sole and exclusive remedy, ServiceNow will refund to Customer any unused prepaid fees.

8.3 LIABILITY. Use of a Sub-Processor will not relieve, waive, or diminish any obligation Data Processor has under the Agreement, and Data Processor is liable for the acts and omissions of any Sub-Processor to the same extent as if the acts or omissions were performed by Data Processor.

9. INTERNATIONAL DATA TRANSFERS

9.1 STANDARD CONTRACTUAL CLAUSES AND ADEQUACY. Where required under Data Protection Laws, Data Processor or Data Processor's Affiliates shall require Sub-Processors to abide by **(a)** the Standard Contractual Clauses for Data Processors established in third countries; or **(b)** another lawful mechanism for the transfer of Personal Data as approved by the European Commission.

9.2 PRIVACY SHIELD. ServiceNow, Inc. shall comply with the EU-U.S. and Swiss-U.S. Privacy Shield Framework set forth by the United States Department of Commerce with respect to the Processing of Personal Data transferred from the European Economic Area and Switzerland to the United States.

///
///
///
Remainder of page intentionally left blank

servicenow

SUBSCRIPTION SERVICE AGREEMENT

APPENDIX 1

DETAILS OF PROCESSING

Nature and Purpose of Processing

Data Processor will Process Personal Data as required to provide the Subscription Service and Professional Services and in accordance with the Agreement.

Duration of Processing

Data Processor will Process Personal Data for the duration of the Agreement and in accordance with Section 4 (Data Processor) of this DPA.

Data Subjects

Data Controller may submit Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller, and may include Personal Data relating to the following categories of Data Subjects:

- clients and other business contacts;
- employees and contractors;
- subcontractors and agents; and
- consultants and partners.

Categories of Personal Data

Data Controller may submit Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller, and may include the following categories:

- communication data (e.g. telephone, email);
- business and personal contact details; and
- other Personal Data submitted to the Subscription Service.

Special Categories of Personal Data

Data Controller may submit Special Categories of Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller in compliance with Data Protection Law, and may include the following categories, if any:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data or biometric data;
- health information; and
- sex life or sexual orientation.

Processing Operations

The personal data transferred will be subject to the following basic processing activities:

- All activities necessary for the performance of the Agreement.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

EXHIBIT A.5 - DATA SECURITY GUIDE

This Data Security Guide forms a part of the Agreement and describes the measures ServiceNow takes to protect Customer Data.

In the event of any conflict between the terms of this Data Security Guide and the terms of the Agreement with respect to the subject matter herein, this Data Security Guide shall control. All capitalized terms not defined in this Data Security Guide will have the meaning given to them in other parts of the Agreement.

1. SECURITY PROGRAM

While providing the Subscription Service, ServiceNow will maintain a written information security program of policies, procedures and controls governing the processing, storage, transmission and security of Customer Data (the "**Security Program**"). The Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. ServiceNow regularly tests, assesses, and evaluates the effectiveness of the Security Program and may periodically review and update the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, although no such update will materially reduce the commitments, protections or overall level of service provided to Customer as described herein.

2. PHYSICAL, TECHNICAL, AND ADMINISTRATIVE SECURITY MEASURES

2.1 PHYSICAL SECURITY MEASURES.

2.1.1. Data Center Facilities. **(a)** Physical access restrictions and monitoring that may include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents (e.g. fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; and **(b)** fire detection and fire suppression systems both localized and throughout the data center floor.

2.1.2. SYSTEMS, MACHINES AND DEVICES. **(a)** Physical protection mechanisms; and **(b)** entry controls to limit physical access.

2.1.3. MEDIA. **(a)** Industry standard destruction of sensitive materials before disposition of media; **(b)** secure safe for storing damaged hard disks prior to physical destruction; and **(c)** physical destruction of all decommissioned hard disks storing Customer Data.

2.2 TECHNICAL SECURITY MEASURES.

2.2.1. ACCESS ADMINISTRATION. Access to the Subscription Service by ServiceNow employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production instances. Access privileges are based on job requirements and are revoked upon termination of employment or consulting relationships. Production infrastructure includes appropriate user account and password controls (e.g., the required use of VPN connections, complex passwords with expiration dates, and a two-factored authenticated connection) and is accessible for administration.

2.2.2. SERVICE ACCESS CONTROL. The Subscription Service provides user and role-based access controls. Customer is responsible for configuring such access controls within its instance.

2.2.3. LOGGING AND MONITORING. The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.

2.2.4. FIREWALL SYSTEM. An industry-standard firewall is installed and managed to protect ServiceNow systems by residing on the network to inspect all ingress connections routed to the ServiceNow environment.

2.2.5. VULNERABILITY MANAGEMENT. ServiceNow conducts periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, ServiceNow will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with ServiceNow's then-current vulnerability management and security patch management standard

operating procedure and only after such patch is tested and determined to be safe for installation in all production systems.

2.2.6. ANTIVIRUS. ServiceNow updates antivirus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.

2.2.7. CHANGE CONTROL. ServiceNow ensures that changes to platform, applications, and production infrastructure are evaluated to minimize risk and are implemented following ServiceNow's standard operating procedure.

2.2.8. DATA SEPARATION. Customer Data shall be maintained within a logical single-tenant architecture on multi-tenant cloud infrastructure that is logically and physically separate from ServiceNow's corporate infrastructure.

2.3 ADMINISTRATIVE SECURITY MEASURES.

2.3.1. DATA CENTER INSPECTIONS. ServiceNow performs routine reviews at each data center to ensure that it continues to maintain the security controls necessary to comply with the Security Program.

2.3.2. PERSONNEL SECURITY. ServiceNow performs background screening on all employees and all contractors who have access to Customer Data in accordance with ServiceNow's then-current applicable standard operating procedure and subject to Law.

2.3.3. SECURITY AWARENESS AND TRAINING. ServiceNow maintains a security awareness program that includes appropriate training of ServiceNow personnel on the Security Program. Training is conducted at time of hire and periodically throughout employment at ServiceNow.

2.3.4. VENDOR RISK MANAGEMENT. ServiceNow maintains a vendor risk management program that assesses all vendors that access, store, process, or transmit Customer Data for appropriate security controls and business disciplines.

3. SERVICE CONTINUITY

3.1 DATA MANAGEMENT; DATA BACKUP. ServiceNow will host Customer's access to and use of purchased instances of the Subscription Service in a pair of data centers that attained SSAE 18 Type 2 attestations or have ISO 27001 certifications (or equivalent or successor attestations) acting in an active/active capacity for the Subscription Term. Each data center includes full redundancy (N+1) and fault tolerant infrastructure for electrical, cooling and network systems. The deployed servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability. The production database servers are replicated in near real time to a mirrored data center in a different geographic region. Each Customer instance is supported by a network configuration with multiple connections to the Internet. ServiceNow backs up all Customer Data in accordance with ServiceNow's standard operating procedure.

3.2 PERSONNEL. In the event of an emergency that renders the customer support telephone system unavailable, all calls are routed to an answering service that will transfer to a ServiceNow telephone support representative, geographically distributed to ensure business continuity for support operations.

4. CERTIFICATIONS AND AUDITS

4.1 CERTIFICATIONS AND ATTESTATIONS. ServiceNow shall establish and maintain sufficient controls to meet the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent standards) (collectively, the "**Standards**") for the information security management system supporting the Subscription Service. At least once per calendar year, ServiceNow shall obtain an assessment against such Standards by an independent third-party auditor.

4.2 CUSTOMER MONITORING RIGHTS.

4.2.1. REMOTE SELF ASSESSMENTS. ServiceNow shall enable remote self-serve assessments of its Security Program by granting Customer, at all times and at no additional costs, access to the ServiceNow self-access documentation portal ("**ServiceNow CORE**"). The information available on ServiceNow CORE will include documentation evidencing ServiceNow's policies, procedures and security measures, as well as copies of the certifications and attestations listed in Section 4.2.2 (Audit) below.

4.2.2. AUDIT. No more than once per year and upon written request by Customer, Customer shall have the right directly or through its representative(s) (provided however, that such representative(s) shall enter into written obligations of confidentiality directly with ServiceNow), to access all reasonable and industry recognized documentation evidencing ServiceNow's policies and procedures governing the security of Customer Data ("**Audit**"). Such Audit shall include a written summary report of any assessment performed by an independent third-party of ServiceNow's information security management system supporting the Subscription Service against the objectives stated in ISO 27001, ISO 27018, SSAE 18 / SOC 1 and SOC 2 Type 2 (or equivalent or successor attestations). ServiceNow reserves the right to refuse to provide Customer (or its representatives) with any information which would pose a security risk to ServiceNow or its customers, or which ServiceNow is prohibited to provide or disclose under Law or contractual obligation.

4.2.3. OUTPUT. Upon completion of the Audit, ServiceNow and Customer may schedule a mutually convenient time to discuss the output of the Audit. ServiceNow may in its sole discretion, consistent with industry and ServiceNow's standards and practices, make commercially reasonable efforts to implement Customer's suggested improvements noted in the Audit to improve ServiceNow's Security Program. The Audit and the results derived therefrom are Confidential Information of ServiceNow.

4.2.4. CUSTOMER EXPENSES. Any expenses incurred by Customer in connection with the Audit shall be borne exclusively by Customer.

5. MONITORING AND INCIDENT MANAGEMENT

5.1 MONITORING, MANAGEMENT AND NOTIFICATION.

5.1.1. INCIDENT MONITORING AND MANAGEMENT. ServiceNow will monitor, analyze, and respond to security incidents in a timely manner in accordance with ServiceNow's standard operating procedure. ServiceNow's security group will escalate and engage response teams as may be necessary to address an incident.

5.1.2. BREACH NOTIFICATION. ServiceNow will report to Customer any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data (a "**Breach**") without undue delay following determination by ServiceNow that a Breach has occurred.

5.1.3. REPORT. The initial report will be made to Customer security or privacy contact(s) designated in ServiceNow's customer support portal (or if no such contact(s) are designated, to the primary contact designated by Customer). As information is collected or otherwise becomes available, ServiceNow shall provide without undue delay any further information regarding the nature and consequences of the Breach to allow Customer to notify relevant parties, including affected Data Subjects, government agencies, and data protection authorities in accordance with Data Protection Laws. The report will include the name and contact information of the ServiceNow contact from whom additional information may be obtained. ServiceNow shall inform Customer of the measures that it will adopt to mitigate the cause of the Breach and to prevent future Breaches.

5.1.4. CUSTOMER OBLIGATIONS. Customer will cooperate with ServiceNow in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, including any Breaches, identify its root cause(s), and prevent a recurrence. Customer is solely responsible for determining whether to notify the relevant supervisory or regulatory authorities and impacted Data Subjects and for providing such notice.

5.2 USE OF AGGREGATE DATA. ServiceNow may collect, use, and disclose quantitative data derived from Customer's use of the Subscription Service for industry analysis, benchmarking, analytics, marketing, and other business purposes in support of the provision of the Subscription Service. Any such data will be in aggregate form only and will not contain Customer Data.

5.3 COOKIES. When providing the Subscription Service, ServiceNow uses cookies to: **(a)** track session state; **(b)** route a browser request to a specific node when multiple nodes are assigned; and **(c)** recognize a user upon returning to the Subscription Service. Customer shall be responsible for providing notice to, and collecting any necessary consents from, its authorized users of the Subscription Service for ServiceNow's use of cookies.

servicenow

SUBSCRIPTION SERVICE AGREEMENT

6. PENETRATION TESTS

6.1 BY A THIRD-PARTY. ServiceNow contracts with third-party vendors to perform a penetration test on the ServiceNow application per family release to identify risks and remediation that help increase security.

6.2 BY CUSTOMER. No more than once per calendar year Customer may request to perform, at its own expense, an application penetration test of a sub-production instance of the Subscription Service. Customer shall notify ServiceNow in advance of any test by submitting a request to schedule an application penetration test using ServiceNow's customer support portal per ServiceNow's then-current penetration testing policy and procedure, including entering into ServiceNow's penetration test agreement. ServiceNow and Customer must agree on a mutually acceptable time for the test; and Customer shall not perform a penetration test without ServiceNow's express written authorization. The test must be of reasonable duration, but in no event longer than 14 days and must not interfere with ServiceNow's day-to-day operations. Promptly on completion of the penetration test, Customer shall provide ServiceNow with the test results including any detected vulnerability. Upon such notice, ServiceNow shall, consistent with industry-standard practices, use all commercially reasonable efforts to promptly make any necessary changes to improve the security of the Subscription Service. Customer shall treat the test results as Confidential Information of ServiceNow subject to the confidentiality requirements in the Agreement.

7. SHARING THE SECURITY RESPONSIBILITY

7.1 PRODUCT CAPABILITIES. The Subscription Service has the capabilities to: **(a)** authenticate users before access; **(b)** encrypt passwords; **(c)** allow users to manage passwords; and **(d)** prevent access by users with an inactive account. Customer manages each user's access to and use of the Subscription Service by assigning to each user a credential and user type that controls the level of access to the Subscription Service. Customer shall be responsible for implementing encryption and access control functionalities available within the Subscription Service for protecting all Customer Data containing sensitive data, including credit card numbers, social security and other government-issued identification numbers, financial and health information, Personal Data, and any Personal Data deemed sensitive or "special categories of personal data" under Data Protection Laws. Customer is solely responsible for its decision not to encrypt such data and ServiceNow will have no liability to the extent that damages would have been mitigated by Customer's use of such encryption measures. Customer is responsible for protecting the confidentiality of each user's login and password and managing each user's access to the Subscription Service.

7.2 CUSTOMER COOPERATION. Customer shall promptly apply any Upgrade or Update that ServiceNow determines is necessary to maintain the security, performance, or availability of the Subscription Service.

7.3 LIMITATIONS. Notwithstanding anything to the contrary in this Data Security Guide or other parts of the Agreement, ServiceNow's obligations extend only to those systems, networks, network devices, facilities, and components over which ServiceNow exercises control. This Data Security Guide does not apply to: **(a)** information shared with ServiceNow that is not Customer Data; **(b)** data in Customer's VPN or a third-party network; **(c)** any data processed by Customer or its users in violation of the Agreement or this Data Security Guide; or **(d)** Integrated Products. For the purposes of this Data Security Guide, "**Integrated Products**" shall mean ServiceNow-provided integrations to third-party products or any other third-party products that are used by Customer in connection with the Subscription Service. Customer agrees that its use of such Integrated Products will be: **(i)** in compliance with all Laws, including but not limited to, Data Protection Laws; and **(ii)** in accordance with its contractual agreement with the provider of such Integrated Products. Any Personal Data populated from the Integrated Products to the Subscription Service must be collected, used, disclosed and, if applicable, internationally transferred in accordance with Customer's privacy policy, which will adhere to Data Protection Laws.

31. APPENDIX: APPDYNAMICS SECURITY AND PRIVACY STANDARD - CONFIDENTIAL

APPDYNAMICS

AppDynamics Security and Privacy Standard

AppDynamics is committed at all levels to the security of Customer Data. AppDynamics has developed a comprehensive security program and organization that is supported by leadership who are committed to proactively managing cyber-security risk. By focusing on a secure-by-design approach, AppDynamics seeks to weave security into its development practices early and layer security across our architecture to protect its corporate services, supply chain, software distribution, and customer-facing services.

AppDynamics' Chief Information Security Officer (CISO) has established this document to provide a general overview of the policies, standards, practices, and procedural controls used to ensure the protection and privacy of our systems, applications, infrastructure, facilities, and personnel. These controls are used to protect Customer Data through the secure development, operation, and maintenance of AppDynamics' products and services.

Additionally, AppDynamics undergoes semi-annual SOC 2 audits. Customers and potential customers may request a copy of the most recent independent auditor's report under a non-disclosure agreement.

Security Program

AppDynamics maintains the Security Program in a manner designed to protect AppDynamics' Information Systems from internal and external security threats, loss, and unauthorized disclosure. AppDynamics' CISO is responsible for the management of information security throughout the company including corporate security, product security, and the security of AppDynamics' SaaS-based customer environments. The Security Program is focused on managing risk as a continuous cycle through three key functions: Security Assurance, Security Engineering, and Security Operations. Each of the functions relies on one another and the broader organization to manage and build effective security controls, quickly detect and respond to incidents, and constantly test ourselves to maintain a healthy operating risk posture for our customers, our company, and our stakeholders.

Chief Information Security Officer - AppDynamics' CISO reports to executive management on information security and is accountable for establishing people, process, and technology controls to manage and communicate the overall state of AppDynamics' security posture to the whole company. The CISO is responsible for AppDynamics' information security policies, standards, and processes and ensuring their effectiveness. As the champion for the development and implementation of security solutions and capabilities throughout the enterprise and within our Software, the CISO works closely with his/her team and other company leaders to continuously manage risk within acceptable thresholds as derived from executive leadership.

Security Assurance - AppDynamics' Security Assurance team creates and maintains AppDynamics' information security policies and maintains an enterprise-wide strategy for the continuous evaluation of AppDynamics' security capabilities. The Security Assurance team is responsible for providing security assessments from products to infrastructure and driving independent attestations of AppDynamics security posture, such as the SOC 2. The Security Assurance team is also responsible for ensuring security compliance and providing guidance on information security risk and any mitigations. In concert with the AppDynamics legal team, Security Assurance monitors industry trends and regulatory changes that could impact information security and privacy. Security Assurance also develops and delivers security awareness training to ensure continuous education as a critical company security control.

Security Engineering - AppDynamics' Security Engineering team is responsible for designing and implementing a standardized set of information security controls and processes across the enterprise. The Security Engineering team partners closely with the engineering and product management teams to ensure that security is a focus throughout the software development lifecycle; with the information technology teams to ensure that information security requirements are addressed; and with the technical operations teams to ensure that SaaS systems are architected and operated in a secure manner.

Security Operations - AppDynamics' Security Operations team is responsible for the day-to-day security "watch" of the Software and Information Systems. The team provides continuous monitoring of the Information Systems and infrastructure that power the AppDynamics business. The Security Operations team utilizes people, process, and technology to proactively stay abreast of emerging threats and vulnerabilities to ensure that AppDynamics is protected. Since no operation is attack-proof, the Security Operations team's focus is to be attack-resilient. The Security Operations team performs active response to and pro-active "hunting" of suspicious alerts, events, and incidents. As the first-responders and incident commanders, the Security Operations team is also responsible for handling communication and rapid mitigation of security incidents. In order to operate effectively and efficiently, the Security Operations team seeks to minimize the time it takes to detect and respond and security alerts, events, and incidents to maintain a healthy environment.

Definitions

AppDynamics Personnel - All employees of AppDynamics and subcontractors engaged by AppDynamics to deliver Services to customers and AppDynamics employees who support the Information Systems.

Customer Data - Any and all data and information that End User configures the Software to collect, which is supplied to AppDynamics in accordance with any agreements between the End User and AppDynamics.

Customer Resources - Customer-owned and managed facilities, systems, and networks, excluding any AppDynamics Information Systems, software-as-a-service (SaaS) infrastructure, or systems otherwise managed by AppDynamics.

Information Systems - AppDynamics' systems and networks that store, process and or transmit Customer Data.

SOC 2 - Service Organization Control (SOC) 2 audit performed in accordance with the AT 101 standards and based upon the Trust Services Principles established by American Institute of Certified Public Accountants that audits the operating effectiveness of AppDynamics' controls (Type II) as they relate to security, availability, and confidentiality.

Software - AppDynamics application intelligence software product(s).

Customer Data

AppDynamics' systems and procedures are designed to protect against the damage, loss or unauthorized access of any Customer Data. AppDynamics has implemented administrative, technical and physical safeguards designed to ensure the confidentiality and integrity of Customer Data. Our servers are protected by physical and electronic security measures, and we leverage data-protection controls such as encryption, data-minimization, and authentication, authorization, and accounting (AAA) (where it is required and technically feasible).

Protection of Customer Data - AppDynamics implements industry standard technical and organizational measures designed to protect Customer Data against unauthorized or unlawful use, and against accidental loss, destruction, or damage. AppDynamics limits access to Customer Data to those AppDynamics Personnel who need to access the Customer

Data for the purposes described here, and such personnel are required to sign agreements with confidentiality protections as part of their employment.

Third Parties - AppDynamics will not disclose Customer Data to any third party except that AppDynamics may disclose such information (a) to an AppDynamics subcontractor or vendor who needs access to assist AppDynamics in providing the Software or Services; (b) with customer's express written permission; or (c) to comply with applicable law. Customer Data is not shared or sold to marketers.

General Security Controls

As part of the Security Program, AppDynamics implements people, process, and technical controls designed to manage cybersecurity risks. Controls may be physical, technical or administrative in their operation, and they may be preventative, detective, corrective, deterrent or recovery focused in their intent. Controls may include hardware and software functions, processes, and procedures, as well as organizational and managerial structures. Controls are reviewed periodically to ensure they are still appropriate.

Policies - AppDynamics maintains internal security policies that are approved by AppDynamics' senior management that are published internally and communicated to AppDynamics Personnel. Policies are reviewed and updated no less than annually to ensure continued applicability with respect to changes in AppDynamics' risk tolerance, the architecture of AppDynamics' products and systems, available technologies, changes to relevant industry standards, such as National Institute of Standards and Technology and International Organization for Standardization, as well as changes to applicable law.

Risk Assessments - AppDynamics performs periodic risk assessments on critical information systems, networks, and applications. Results of the assessments are documented, reviewed with the system owner, and remediations for any identified gaps are prioritized.

Vendor Due Diligence - Prior to engaging with any third party that accesses production infrastructure or processes Customer Data, AppDynamics performs appropriate due diligence to ensure that the third party's information security program is reasonable and consistent with AppDynamics' obligations to the scope of the engagement and the types of data under the control or accessible by the third party.

Credentials - AppDynamics maintains a credential policy that sets minimum standards appropriate for the systems being secured including complexity requirements for passwords and minimum key lengths. AppDynamics leverages multi-factor authentication for access to Information Systems. Any privileged credentials such as root keys and service account credentials are stored securely and are rotated upon the departure of personnel with knowledge of these credentials in the absence of any mitigating controls.

Access Control - AppDynamics uses industry-standard techniques designed to restrict access to and to prevent unauthorized use of its Information Systems. AppDynamics requires the use of individual user accounts to maintain the integrity of audit trails. User and group management is centralized using single-sign-on systems and access to systems is subject to management approval. Access to sensitive systems, including all systems that process or store Customer Data is reviewed and re-approval is required periodically.

Role-Based Access - AppDynamics follows the principle of least privilege and, where possible, employs segregation of duties and dual knowledge principles. System owners maintain access control policies, procedures, and documentation for each system including the privileges assigned to users and groups.

Anti-Malware - AppDynamics employs appropriate anti-malware software on Information Systems. The anti-malware software is centrally managed and configured to allow for automatic updates.

Change Management - All changes to AppDynamics Information Systems in production environments, including network and other infrastructure, are authorized, tracked, tested, and monitored. Where AppDynamics utilizes configuration management or infrastructure-as-code changes undergo peer code review prior to being deployed.

Logging - Logs from systems and applications, including network devices and firewalls, are forwarded to centralized logging infrastructure that is configured to alert when specific or anomalous events are detected. Such logs are secured to prevent tampering and are retained for an appropriate amount of time that allows for after-the-fact investigations.

Monitoring - AppDynamics monitors the Information Systems as well as the underlying infrastructure on a 24x7x365 basis and maintains an on-call rotation of qualified personnel who are notified immediately of any failures or material degradations of service.

Business Continuity - AppDynamics maintains a business continuity plan designed to minimize the impact to business operations of potential threats. The plan is sponsored by executive management and reviewed on an annual basis. AppDynamics performs exercises of various scenarios as well as tabletop exercises of more complex scenarios on a periodic basis.

Backups and Disaster Recovery - AppDynamics maintains disaster recovery plans for its Information Systems. Backup frequency and retention period is system specific and determined by the classification of the system. For Information Systems hosting the SaaS version of the Software, backups are taken daily and transferred off-site on a weekly basis. Backups are tested regularly and restore procedures are validated to ensure that data can be restored.

Network Security - AppDynamics employs a defense-in-depth strategy for network security including the use of perimeter, host-based, and web-application firewalls, physical segregation of development and production environments, and network access control lists between subnets. Firewall configurations are maintained under change control processes and procedures and are reviewed periodically.

Denial of Service - AppDynamics has engaged a leading provider of Denial of Service (DoS) and Distributed Denial of Service (DDoS) mitigation to protect its SaaS-based environments. AppDynamics also implements request rate-limiting at service endpoints and has implemented controls to protect resources shared between customers.

Encryption - All AppDynamics Software supports encryption. AppDynamics strongly encourages end users of the Software to ensure that agents are configured to communicate to the controller software using SSL/TLS. Additionally, AppDynamics utilizes encrypted connections for inter-tier communications that occur over non-AppDynamics controlled networks. The method of encryption varies based on the protocol of the communication but meets or exceeds industry standards established for the method in use.

Data Destruction - AppDynamics securely erases or destroys all media that contains Customer Data prior to reuse outside of the production environment using industry-standard procedures.

Managing Vulnerabilities

AppDynamics follows a risk-based methodology leveraging relevant industry standards, such as CVSS, to prioritize security issues based on their impact severity and likelihood of exploitation. AppDynamics aims to release patches or remediate an issue in a reasonable period of time commensurate with the results of the risk assessment. Generally, higher-impact issues will be prioritized and fixed sooner than lower-impact issues. However, the exact amount of time required to fix a vulnerability is unique to each finding and depends on a set of factors, including the complexity of the issue, the number of components impacted, and any third party dependencies.

Responsible Disclosure - AppDynamics follows a responsible disclosure model for reporting vulnerabilities in the Software and infrastructure. Reporters may submit any issues or concerns to *security@appdynamics.com* . Further communication or updates are available at *https://www.appdynamics.com/security* .

Product Vulnerabilities - It is AppDynamics' intent to discover and remediate vulnerabilities in its Software prior to release. In order to accomplish this, AppDynamics utilizes industry-standard techniques as part of its software development life cycle. Such techniques include peer code review prior to merge; static code analysis; malware scans of build artifacts; and scans of third party libraries and dependencies for known vulnerabilities against the NIST National Vulnerability Database (*https://nvd.nist.gov*).

Infrastructure Vulnerabilities - AppDynamics' vulnerability management program is designed to detect vulnerabilities all at layers of AppDynamics' Information Systems using industry-standard tools and track identified vulnerabilities until remediation. AppDynamics subscribes to notification channels for its vendors as well as industry feeds for vulnerabilities.

Customer Notification - Once a fix is available, AppDynamics provides notification to affected customers based on the risk of the vulnerability. Depending on the severity, notifications to customers may be issued through multiple channels including AppDynamics customer portal, email, or product release notes.

Third Party Assessments - AppDynamics regularly engages qualified third parties to perform independent assessments of AppDynamics' source code, products, and infrastructure.

Incident Response

AppDynamics maintains an Incident Response Policy and trains all personnel identified in the policy of their responsibilities on a semi-annual basis. In the event of a suspected incident the incident response team is notified and immediately begins a reasonable investigation as to whether or not a breach has occurred. In the event of a reasonably suspected breach, AppDynamics will use commercially reasonable efforts to contain, mitigate, and resolve the breach as well as put in place additional controls to prevent further breaches of a similar type.

AppDynamics has retained a leading incident response provider to provide additional incident response capabilities and reserves the right to engage their services without prior approval from affected customers.

Notification - Where allowed by applicable law, AppDynamics will promptly notify affected customers of a security incident that affects Customer Data. Once AppDynamics has reasonably determined that Customer Data has been impacted, AppDynamics will promptly notify the impacted customer(s) following such determination. In accordance with its Incident Response Policy, AppDynamics will provide reasonable details regarding the incident, the steps taken by AppDynamics to contain, mitigate, resolve, and prevent future incidents provided that, in AppDynamics' sole discretion, such information does not impact the confidentiality of other AppDynamics customers or the overall security posture of AppDynamics.

AppDynamics, in its sole discretion, may publicly disclose the fact that a security incident has occurred but will not name affected customers. Additionally, in accordance with its Information Security Policy, AppDynamics may notify local, state, federal, and or international law enforcement agencies.

Personnel Controls

All AppDynamics Personnel are required to adhere to confidentiality obligations under their contracts of employment or engagement. Additionally, all AppDynamics Personnel are required to adhere to AppDynamics' policies and procedures

and acknowledge their understanding that violation of AppDynamics' policies is subject to disciplinary action up to and including termination.

Background Checks - Prior to employment, all AppDynamics employees are required to submit to background checks. Such checks are performed by an industry-leading provider to perform criminal and overall background screening services. On completion, the results are provided to AppDynamics and reviewed by AppDynamics' Human Resources team who determine if the results contain any red flags that may require further investigation or adverse action.

For AppDynamics employees located in the United States, background investigations include the following, where allowed by law: (1) SSN Trace; (2) Criminal County Search; (3) Multi-state and Federal Criminal Record Search; (4) National Sex Offender Registry Search; (5) Global Sanctions and Enforcement; (6) Education Verification; (7) Employment; (8) International Criminal Search.

Outside of the United States, AppDynamics requires all employees to submit to the highest degree of criminal background checks and screening that is allowed by local law.

Training - All AppDynamics employees are required to undergo annual training. The contents of such training is dependent on a person's role but includes human resources training, legal and confidentiality training, and security awareness training.

Termination - Upon termination of a relationship with AppDynamics, all AppDynamics Personnel are required to turn over all AppDynamics equipment in their possession. System access is revoked within 24 hours of separation.

Qualifications - Prior to entering into an employment or other relationship with AppDynamics, all AppDynamics Personnel are interviewed and qualifications evaluated to ensure that candidates are qualified and capable of performing the required functions as described in the job description.

Customer Resources

AppDynamics is committed to following relevant customer policies and procedures when accessing Customer Resources.

Policies - AppDynamics Personnel will follow relevant customer policies and procedures that are provided to AppDynamics when onsite at customer facilities and when leveraging Customer Resources. It is the responsibility of the customer to provide reasonable notice of the content of any such policies and procedures, and appropriate training where required, to AppDynamics Personnel with such access.

Customer Resources - AppDynamics Personnel will not access Customer Resources or facilities without permission from the customer. Customers may revoke such permission at any time with written notice although this may delay the delivery of any Services. AppDynamics is responsible for all uses of Customer Resources by AppDynamics Personnel.

Customer Devices - AppDynamics will not copy or install any software onto a Customer Resource without permission from the customer. If AppDynamics is in possession of any Customer Resource, AppDynamics will take appropriate measures designed to secure such devices, using methods and protocols no less protective than those AppDynamics uses to secure its own similar devices. AppDynamics will promptly return any Customer Resources in its possession to the customer upon request.

32. APPENDIX: RRMS SLA AND AGREEMENT SAMPLE

Red River [redacted]

1. INTRODUCTION

Red River is pleased to provide this statement of work to [redacted] This document specifies the scope and schedule of the services delivered to the end customer by Red River Managed Services under the Red River Managed Services Support Contract. This package is customized to provide [redacted] with a comprehensive support solution.

The purpose of this document is to provide a detailed description of the services delivered by Red River Managed Services available through this statement of work. As a requirement to initiate Red River Managed Services, this document must be signed by both parties as an agreement for the scope and deliverables of the services under this statement of work.

2. DETAILED SCOPE OF SERVICES

This document specifies the scope and schedule of the services to be delivered, lists the devices for which support is provided, and defines the alignment of services and schedules of services to specific supported devices. This document also identifies guidelines and procedures for providing support and service to the end customers by determining priority, issue resolution and communication of updates to the statement of work.

The services listed in the table below are included within this statement of work. Additional details regarding these services are included in the subsections within Section 2.

2.1 Summary of Included Services

Remote NOC support labor will be provided utilizing a monthly allotment of service hours. Overages will be applied as needed. Section 2.2 includes additional details about the allotment of service hours as well as the services listed below.

Table 1 - Included Services

Process or Service Area	Services & Tasks	Fixed Price	Service Hours
Incident Management	Level I Help Desk and triage to [redacted] on-call resources		•
	Remote troubleshooting (Up to 20 minutes per ticket as requested by [redacted]		•
	Escalation to [redacted] per [redacted] SLA Matrix		•
Problem Management	Root cause analysis & problem resolution		•
Change Management	Documentation and execution of changes to managed configuration items		•
	Windows Server Patching		•
Request Fulfillment	Standard requests for Moves, Adds, Deletions		•
Customer Success Management	Monthly Checkpoint Calls	•	
	Monthly Ticket Reports	•	
	Quarterly Business Reviews	•	

[redacted]

April 16, 2018 - 2 - Version No. 2

Red River®

[redacted]

2.2 Remote NOC Support

Red River's US-based Network Operation Center (NOC), headquartered in Claremont, New Hampshire, is staffed 24 hours per day, every day of the week and year. The services described in this Section 2.2 will be delivered by Red River's NOC using a monthly allotment of service hours.

This agreement includes a monthly allotment of service hours, with 100 percent cumulative rollover, and a monthly usage cap. Overages will be applied when usage exceeds the available service hours or the monthly usage cap.

Monthly Allotment of Service Hours

Service Hours per Month:	**50**
100% Rollover:	Cumulative
Monthly Usage Cap:	60

100% Cumulative Rollover

At the end of each month, all unused service hours will be rolled over and added to the next month's allotment of service hours. Rollover is cumulative for the duration of this agreement, however any remaining service hours at the end of this agreement may not be carried over to a renewal or extension.

Monthly Usage Cap

Regardless of the quantity of accumulated rollover hours, all hours used over 60 in any given month will be billed as overages. Any remaining unused service hours will be rolled over to the next month.

2.2.1 Incident Management

Hypertherm, Inc. may escalate incidents to Red River's NOC for additional troubleshooting and incident management. Incident tickets may be opened via phone, email, or web portal. When reporting a high priority or critical incident, the customer will open the ticket via phone.

2.2.1.1 Incident Classification

Priority	Response SLA	Description
P1: Critical Must be Reported to NOC via Phone	2 Hours	This is an EMERGENCY condition that significantly restricts the use of an application, system or network to perform any critical business function. This could mean that several departments of the customer are impacted.
P2: High Must be Reported to NOC via Phone	4 Hours	The reported issue may severely restrict use of key devices in the network. This could mean that a single department is impacted but the overall network and servers are functioning
P3: Medium	8 Hours	The reported issue may restrict the use of one or more features of the system, but the business or financial impact is not severe.
P4: Low	24 Hours	The reported anomaly in the system does not substantially restrict the use of one or more features of the product to perform necessary business functions.

[redacted]

Red River [redacted]

Escalation Matrix

All alerts will be captured by the customer. Red River will provide ticketing, troubleshooting, and escalation to designated customer contacts.

- Any documented Standard Operation Procedure will be executed by first level of support for verification
- Tickets without SOPs will be escalated to Red River Level 2 Support Team for verification, analysis, and troubleshooting of issues
- Unresolved tickets will be escalated to [redacted] ticketing system or on-call team for additional troubleshooting and resolution. Red River will escalate tickets per the priority definitions of [redacted] SLA matrix.

2.2.2 Problem Management

Hypertherm, Inc. may escalate to the NOC for root cause analysis to identify the underlying problem causing a given incident or incidents. Upon identifying the problem, Red River may propose a change to resolve the problem. [redacted] may approve and assign the change to Red River for completion.

Problem Management tasks include:

- Analyze one or more related incidents to identify underlying causes
- Log, categorize, and diagnose problems
- Identify workarounds (if not already identified during incident management)
- Transfer problems into "known errors"
- Identify solution to problem
- Propose change to resolve problem
- Upon approval, implement change proposal to resolve problem

Depending upon the impact and cost associated with resolving a problem, the customer may not always elect to have the problem resolved. In such cases, the "known errors" entry will include workarounds to resolve related incidents and will state that permanent resolution of the problem is not currently justified.

2.2.3 Change Management

Red River Managed Services documents requests for change in Change Controls which must be reviewed and approved prior to execution. Approvers include the NOC Manager, Customer Success Manager, designated Subject Matter Experts, and customer-appointed resources.

The Change Management process applies to all changes which could affect or interrupt an IT service. Such changes include but are not limited to software updates and patches, configuration changes, and problem resolutions.

Change controls typically include the following information:

- Overview of change to be made
- Impacted systems
- Test and development plan
- Change plan details
- User acceptance test plan
- Schedule

[redacted]

April 16, 2018 - 4 - Version No. 2

Red River [redacted]

- Rollback options

The Customer Success Manager will review the Change Management process with the customer and will define any exceptions which will need to be made in the event of an emergency change.

Windows Server Patch Management

The services described in this section pertain only to servers running Windows operating systems currently supported by Microsoft. Red River Managed Services will remotely provide the following once per month for each server:

- Security and critical updates
- Zero-day fixes
- Up to one hour remote troubleshooting following patching if needed

Backup and restoration of physical servers is the responsibility of the customer. If necessary, Red River Managed Services will work with the customer to schedule physical server backups prior to patching.

Red River will prepare a server patching Standard Operation Procedure (SOP) to be reviewed and approved by [redacted] The SOP may be revised with approval from Red River and [redacted] as needed.

2.2.4 Request Fulfillment

[redacted] may initiate service requests in the same ways they open incident tickets, via email, web portal, or by calling the NOC. Service requests will be processed according to pre-defined standard operating procedures when applicable. All requests, approved or otherwise, will be logged in Red River's ticketing system.

2.3 Customer Success Management

Red River will assign a Customer Success Manager (CSM) to facilitate the operational services and serve as [redacted] primary point of contact for customer service matters. The CSM may hold monthly checkpoint calls with the assigned points of contact to review open tickets and ongoing or upcoming projects.

2.3.1 Quarterly Business Reviews

Four times per year, the CSM will coordinate Quarterly Business Reviews with the customer and other Red River personnel such as the customer Account Executive, a Solutions Architect, and other staff from Managed Services. Red River will assess the business risks, cost containment, and overall customer satisfaction by reviewing base metrics and key performance indicators for the managed devices and services in this SOW. In order to ensure coordination all Red River activities, project updates and future project schedules will be reviewed. Red River will also discuss strategic planning related to demand management and capacity planning trends to ensure supported IT environments can scale to meet your evolving business needs.

2.4 Tasks that are Out of Scope

The following tasks are excluded from the scope of work. (A quote for this work may be provided if requested by customer)

- Site Assessment or Audit

[redacted]

Red River [redacted]

- Onsite Support
- Hardware and/or software warranties or maintenance contract
- Application patching
- Patching for any operating system not currently supported by Microsoft
- Monitoring and alert management

3. ASSUMPTIONS

3.1 Customer Responsibilities

- Provide remote (SSH, telnet, RDP) and/or OOB access to devices to Red River Managed Services, including unique Red River credentials for management of all supported CIs.
- Provide IP addresses and ports of items and nodes to be monitored by Red River's NOC.
- Provide VPN access and unique Red River credentials to Red River's NOC.
- Supply Red River's NOC with administrative credentials for each configuration item to be managed by Red River.
- Provide onsite personnel as needed to assist Red River Managed Services in simple, non-technical assistance.
- Communicate changes or new implementations to be performed on supported devices. Changes, replacements, and decommissioning of supported configuration items must be reported by opening a ticket with Red River's NOC.
- Assure availability of site connectivity 24/7 and manage Internet Service Providers, unless transport CIs are specifically added to this SOW.
- Provide Red River with all necessary information concerning all security considerations and the process Red River should follow to work within any present security policies and processes.

[redacted]

April 16, 2018 - 6 - Version No. 2

Red River®

[redacted]

4. PRICING BREAKDOWN

Item No.	Quantity	Description	Unit Price	Extended Price
RRMS-MR	12	MANAGED SERVICES MONTHLY FEE	$4,210.00	$50,520.00
RRMS-OV	0	MS OVERAGE PER HOUR	$140.00	$0.00
		Total Estimated Price for 1 year:		$50,520.00

Terms

- No setup applies to this statement of work. All labor required to initialize services will be performed utilizing the allotment of service units.
- Contract is 1 year in duration from May 1, 2018 through April 30, 2019. All service hours included in this SOW are valid only during this term. Unused service hours will expire with this SOW.
- Monthly rate will be invoiced at the beginning of each month prior to service. Incremental fees (overages) will be invoiced each month as needed, following service.
- On-Demand Tickets open and closed, Interim Hours usage reports will be provided by Red River upon request.
- Payment terms are Net-30 days from RED RIVER invoice date, a 5% penalty will be applied to late payments.

[redacted]

Red River®

[redacted]

5. TERMINATION

Either party may terminate this SOW in the event that the other party breaches any material obligation under this SOW and fails to cure such breach within thirty (30) days after receiving written notification via certified mail, return receipt requested or by email with confirmed delivery of the particulars of such breach, or other cure period as agreed by both parties. The non-breaching party shall have the right, at its option, to terminate immediately and seek any or all remedies available at law or in equity; or the other party becomes insolvent, makes a general assignment for the benefit of creditors, files a voluntary petition of bankruptcy, suffers or permits the appointment of a receiver for its business assets or become subject to any proceeding under a bankruptcy or insolvency law, domestic or foreign.

This Agreement and all rights and duties hereunder shall terminate upon the happening of the earliest of any of the following:

1.1. The bankruptcy, insolvency, reorganization under the bankruptcy laws, or assignment for the benefit of creditors by either party;

1.2. The sanctioning, suspension or debarment by the Government of either party;

1.3. The mutual consent of both parties in writing.

1.4. In the event the SOW is terminated as a result of Customer breach, Customer shall pay Red River, at a minimum for:

1.4.1. all service provided and undisputed expenses incurred up to the effective date of termination, in accordance with the applicable SOW; PLUS

1.4.2. any additional direct costs which Red River reasonably incurs, such as costs of terminating contractual obligations.

If the SOW is terminated as a result of Red River breach, no further fees incurred after the date of breach, are owed by Customer.

Red River reserves the right to continue billing for services provided after the agreement end date so long as services continue to be delivered by mutual agreement between Customer and Red River.

[redacted]

Red River®

[redacted]

6. POINTS OF CONTACT

The following individuals are designated as the primary points of contacts for receipt of official notices under this Agreement:

Red River Technology LLC

Compliance
21 Water Street – Suite 500
Claremont, New Hampshire 03743
compliance@redriver.com

[redacted]

Miscellaneous

a) This Agreement is the entire Agreement between the parties and supersedes all prior oral or written agreements, commitments, understanding or communications with respect to the subject matter of this Agreement. This Agreement may not be modified except in writing, signed by both parties.

b) Neither Party may assign its rights under this terms and condition without the other Party's prior written consent, which will not be unreasonably withheld or delayed.

c) The invalidity or unenforceability of any provision of these terms and conditions or portion of a provision shall not affect the validity or enforceability of any other provision of these terms and conditions or the remaining portion of the applicable provision.

d) The validity, construction, scope and performance of this Agreement shall be governed by the laws of the State of New Hampshire, without giving effect to any choice of law rules that may require the application of the laws of another jurisdiction, except as to any provisions of this Agreement which are governed by the laws of the United States of America, as to which provisions such laws of the United States shall govern.

[redacted]

Red River®

[redacted]

7. APPROVAL TO PROCEED WITH SERVICE

Following receipt of signed Contract Agreement and Customer's Purchase Order, a RED RIVER Project Manager will contact Customer to discuss next steps. RED RIVER requires a minimum of two (2) weeks' notice to begin support from date of receipt of signed Contract Agreement and Customer's Purchase Order. RED RIVER price quote is valid for thirty (30) days from date of this Statement of Work.

The undersigned parties understand and agree that this SOW accurately sets forth the services that RED RIVER will provide for Customer and that each signer is authorized to accept on behalf of their organization.

Red River Technology LLC

By: Digitally signed by Knowlton.Joanne.M.DRC1000046678.ID DN: c=US, o=U.S. Government, ou=ECA, ou=DRC, ou=Red River Computer Co. Inc., cn=Knowlton.Joanne.M.DRC1000046678.ID Date: 2018.04.24 15:20:49 -04'00'

Name: Joanne Knowlton

Title: Compliance Officer

Date: 4/24/18

[redacted]

[redacted]

Red River [redacted]

8. APPENDIX A – APPROVED CONTACT LIST

All users from [redacted] are authorized to open tickets with Red River's Help Desk.

9. APPENDIX B – CHANGE ORDER FORM

The following form is to be used in the event of required changes to the statement of work. These changes may include added support hours or added devices under the statement of work.

Change to statement of work # RRMS-[redacted]

Quantity Change	Details	Price

[redacted]

Red River Technology LLC Date

[redacted]

Attachment E – Service offering EULAs, SLAs

RESERVED